James E. Cecchi
CARELLA BYRNE CECCHI
OLSTEIN BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, NJ 07068
(973) 994-1700
Lead Counsel for Plaintiffs
(Additional Counsel on the Signature Page)

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

IN RE: AMERICAN MEDICAL COLLECTION AGENCY, INC. CUSTOMER DATA SECURITY BREACH LITIGATION This Document Relates To: All Actions Against Quest Diagnostics, Inc. and Optum360 LLC	Civil Action No. 19-md-2904 (MCA)(MAH) **CONSOLIDATED CLASS ACTION COMPLAINT: QUEST & OPTUM360**

TABLE OF CONTENTS

TABLE OF CONTENTS
(Cont'd)

Page

TABLE OF CONTENTS
(Cont'd)

TABLE OF CONTENTS
(Cont'd)

TABLE OF CONTENTS
(Cont'd)

Plaintiffs, individually on behalf of a class of all those similarly situated (the "Class" or "Class Members"), upon personal knowledge of the facts pertaining to Plaintiffs and on information and belief as to all other matters, and upon the investigation conducted by Plaintiffs' counsel, complain against Defendants, and allege on information and belief as follows:

PRELIMINARY STATEMENT

1. On June 3, 2019, Defendant Quest Diagnostics Inc. ("Quest") revealed in a securities filing that an unauthorized user accessed the system run by Quest's billing collections vendor, Retrieval-Masters Creditor's Bureau, Inc., d/b/a American Medical Collection Agency ("AMCA"), for over six months between late 2018 and March 2019 (the "Data Breach"). After accessing AMCA's systems, the hacker exfiltrated the sensitive personal, financial, and health information of millions of Quest patients and sold the information for profit on underground websites known as the "dark web."

2. Quest contracted with AMCA through 2016 at which point Defendant Optum360 LLC ("Optum360") was assigned that contract pursuant to its work as a revenue cycle management company for Quest.

3. Defendants could have prevented this theft had it limited the customer information they shared with their vendors and business associates and employed reasonable measures to assure their vendors and business associates implemented and maintained adequate data security measures and protocols in order to secure and protect Quest customers' data.

4. Plaintiffs bring this class action because Defendants failed to secure and safeguard Quest patients' protected health information ("PHI") and personally identifiable information ("PII")—such as Plaintiffs' and Class Members' names, mailing addresses, phone numbers, email addresses, dates of birth, Social Security numbers, genders, information related to Plaintiffs' and

Class Members' medical providers and services (such as dates of service, name of lab, referring doctor, test names, internal patient identification number), diagnosis codes, and other personal information—such as credit and debit card numbers, bank account information, and insurance policy numbers (all collectively referred to as "Personal Information").

5. As of today, more than 11.5 million Quest patients have had their Personal Information compromised as a result of the Data Breach. As a result of Defendants' failure to protect the consumer information they were entrusted to safeguard, Plaintiffs and Class Members suffered a loss of value of their Personal Information—and have been exposed to or are at imminent and significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future. In fact, some Class Members' identities have already been stolen.

6. Defendants' intentional, willful, reckless, and negligent conduct—failing to prevent the breach, failing to limit its severity, and failing to detect it in a timely fashion—damaged Plaintiffs uniformly. As discussed herein, fraudulent activities have already been linked to Defendants' conduct. For this reason, Defendants should pay for monetary damages, for appropriate identity theft protection services, and reimburse Plaintiffs for the costs caused by Quest's substandard security practices and failure to timely disclose the same. Plaintiffs are likewise entitled to injunctive and other equitable relief that safeguards their information, requires Defendants to significantly improve their data security, and provides independent, expert oversight of Defendants' security systems.

JURISDICTION AND VENUE

7. This Consolidated Complaint is intended to serve as an administrative summary as to all other complaints consolidated in this multidistrict litigation asserting claims against Quest and Optum360 and shall serve for all purposes as an administrative device to aid efficiency and

economy for the Class defined below. As set forth herein, this Court has general jurisdiction over Defendants and original jurisdiction over Plaintiffs' claims.

8. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, there are more than 100 proposed Class Members, and minimal diversity exists as Defendants are citizens of States different from that of at least one Class member.

9. This Court has personal jurisdiction over Quest because it maintains its principal place of business in this District. Quest is authorized to and regularly conducts business in New Jersey. Quest makes decisions regarding corporate governance and management of its blood testing labs in this District, including decisions regarding the security measures to protect its customers' Personal Information. Quest owns and operates many blood testing labs throughout New Jersey and the United States.

10. This Court has personal jurisdiction over Optum360 because it is authorized and regularly conducts business in New Jersey and has sufficient minimum contacts in New Jersey such that Optum360 intentionally avails itself of this Court's jurisdiction by conducting operations here and contracts with companies in this District.

11. Venue is proper in this District pursuant to 28 U.S.C. § 1407 and the July 31, 2019 Transfer Order of the Judicial Panel on Multidistrict Litigation in MDL 2904 or, in the alternative, pursuant to 28 U.S.C. § 1391 because each of the Defendants transact business and may be found in this District. Specifically, Quest's principal place of business is located in this District and substantial parts of the events or omissions giving rise to the claims occurred in or emanated from this District, including, without limitation, decisions made by Defendants' governance and

management personnel or inaction by those individuals that led to misrepresentations, invasions of privacy, and the data breach.

NAMED PLAINTIFFS

12. Plaintiffs are individuals who, upon information and belief, had their Personal Information compromised in the Data Breach, and bring this action on behalf of themselves and all those similarly situated both across the United States and within their state or territory of residence. These allegations are made upon information and belief derived from, *inter alia*, counsel's investigation, public sources—including sworn statements, Defendants' websites, and the facts and circumstances currently known. Because Defendants have exclusive but perhaps incomplete knowledge of what information was compromised for each individual, including PHI, Plaintiffs reserve the right to supplement their allegations with additional Plaintiffs, facts and injuries as they are discovered.

I. ARKANSAS

A. Plaintiff Ella Gulley

13. Plaintiff Ella Gulley is a citizen and resident of Arkansas.

14. Ella Gulley was a Quest patient who went to obtained blood testing at a Quest laboratory.

15. Ella Gulley provided Quest with her Personal Information as part of obtaining blood testing.

16. Ella Gulley's bill from Quest was subsequently sent to Defendants' billing collections vendor, AMCA.

17. As part of billing collection services provided for Defendants, Ella Gulley has been contacted through several letters, and in response, provided Personal Information to AMCA.

18. As a Quest patient, Ella Gulley believed that Quest would protect her Personal Information once she provided it to Quest or its vendors.

19. Ella Gulley would not have provided Quest with this Personal Information nor used Quest to provide blood testing had she known that it would fail to protect her Personal Information.

20. Ella Gulley suffered and will continue to suffer damages due to the Data Breach.

II. CALIFORNIA

A. Plaintiff Julio Antonio Perez Vieyra

21. Plaintiff Julio Antonio Perez Vieyra is a citizen and resident of California.

22. Plaintiff Vieyra was a Quest patient who went to a Quest laboratory to obtain blood testing services.

23. For years, Plaintiff Vieyra used Quest regularly for routine laboratory testing.

24. Plaintiff Vieyra reviewed and agreed to Quest's privacy policies prior to agreeing to obtain blood testing services.

25. Plaintiff Vieyra provided Quest with his Personal Information as part of obtaining blood testing, including his address, date of birth, Social Security number, and driver's license number.

26. Plaintiff Vieyra's bill from Quest was subsequently sent to AMCA.

27. Plaintiff Vieyra remains in collections with Quest.

28. In response to the Data Breach, Plaintiff Vieyra has begun carefully reviewing his financial and medical accounts to guard against fraud. Plaintiff Vieyra spends three hours every week monitoring his accounts for fraudulent activity.

29. In October 2019, Plaintiff Vieyra identified a fraudulent charge on his bank account and spent four hours attempting to contact his bank to alert them of the fraud.

30. As a Quest patient, Plaintiff Vieyra believed that Quest would protect his Personal Information once he provided it to Quest.

31. Plaintiff Vieyra would not have provided Quest with his Personal Information nor used Quest to provide blood testing had he known that it would fail to protect his Personal Information.

32. Plaintiff Vieyra suffered and will continue to suffer damages due to the Data Breach.

III. COLORADO

A. Plaintiff Moises Perez

33. Plaintiff Moises Perez is a citizen and resident of Colorado.

34. Plaintiff Perez was a Quest patient who went to a Quest laboratory to obtain blood testing services.

35. Plaintiff Perez provided Quest with his Personal Information as part of obtaining blood testing.

36. Plaintiff Perez unpaid bill from Quest was subsequently sent to AMCA.

37. Plaintiff Perez received a collections notice from AMCA dated April 28, 2014, stating that AMCA was pursuing collection of a $20.25 debt he owed to Quest.

38. Plaintiff Perez received a letter from AMCA dated June 4, 2019 informing him that his Personal Information including his "first and last name, name of lab or medical service provider, date of medical service, referring doctor, [and] certain other medical information" was at risk due to the Data Breach.

39. Following the Data Breach, Plaintiff Perez spent two hours trying to reach AMCA for information regarding the Data Breach.

40. In response to the Data Breach, Plaintiff Perez took measures to protect himself, including spending 20 hours monitoring his financial accounts and credit score for fraudulent activity.

41. As a Quest patient, Plaintiff Perez believed that Quest would protect his Personal Information once he provided it to Quest.

42. Plaintiff Perez would not have provided Quest with his Personal Information nor used Quest for testing had he known that it would fail to protect his Personal Information.

43. Plaintiff Perez suffered and will continue to suffer damages due to the Data Breach.

IV. FLORIDA

A. Plaintiff Noel Benadom

44. Plaintiff Noel Benadom is a citizen and resident of Florida.

45. Plaintiff Benadom was a Quest patient who went to a Quest laboratory to obtain blood testing services.

46. Plaintiff Benadom reviewed and agreed to Quest's privacy policies prior to agreeing to obtain blood testing services.

47. Plaintiff Benadom provided Quest with his Personal Information as part of obtaining blood testing.

48. Plaintiff Benadom's bill from Quest was subsequently sent to AMCA.

49. AMCA notified Plaintiff Benadom via letter dated June 4, 2019 of the Data Breach.

50. AMCA informed Plaintiff Benadom that information including his first and last name, his Social Security Number, the name of his lab or medical service provider, the date of his medical service, his referring doctor and other medical information may have been stored on AMCA's system that was compromised.

51. As a result of the data breach, on May 20, 2019, an unauthorized charge to Plaintiff Benadom's Orbitz.com travel account was subject to unauthorized access.

52. On May 21, 2019, Orbitz.com confirmed that an unauthorized individual attempted to book a $125 ticket to Universal Studios Hollywood on Plaintiff Benadom's credit card.

53. Plaintiff Benadom spent more than one hour addressing the identity theft with Orbitz.com.

54. Plaintiff Benadom began regularly monitoring his financial accounts and obtained identify theft protection and credit monitoring services from Capital One and ID Me after learning of the data breach.

55. As a Quest patient, Plaintiff Benadom believed that Quest would protect his Personal Information once he provided it to Quest.

56. Plaintiff Benadom would have sought an alternative medical testing facility had he known that Quest would not protect his Personal Information.

57. Plaintiff Benadom suffered and will continue to suffer damages due to the Data Breach.

B. Plaintiffs Nancy and William Infield

58. Plaintiffs Nancy and William Infield are citizens and residents of Florida.

59. Plaintiffs Nancy and William Infield were Quest patients who went to a Quest laboratory to obtain blood testing services in at least 2013 and 2018.

60. Plaintiffs Nancy and William Infield provided Quest with their Personal Information as part of obtaining blood testing.

61. Plaintiffs Nancy and William Infield both had unpaid bills from Quest, which were subsequently sent to AMCA.

62. Plaintiff William Infield received a collections notice from AMCA dated May 15, 2019, stating that AMCA was pursuing collection of a $25.76 debt he owed to Quest.

63. Plaintiff William Infield received a letter from AMCA dated June 6, 2019 informing him that his Personal Information including his "first and last name, name of lab or medical service provider, date of medical service, referring doctor, [and] certain other medical information" was at risk due to the Data Breach.

64. Plaintiff Nancy Infield received three separate letters from AMCA, all dated June 6, 2019, informing her that her Personal Information including her "first and last name, Social Security number, name of lab or medical service provider, date of medical service, referring doctor, [and] certain other medical information" was at risk due to the Data Breach.

65. In October 2019, Plaintiff Nancy Infield called AMCA and was told that the bill she was in collections for was owed to Quest.

66. Following the Data Breach, Plaintiff Nancy Infield began receiving suspicious phishing calls. The callers have her name, address, and last four digits of her Social Security number. She receives several calls per month. She has reported the calls to the Federal Trade Commission.

67. In response to the Data Breach, Plaintiffs Nancy and William Infield took mitigative measures, including spending substantial time monitoring their accounts for fraudulent activity.

68. As Quest patients, Plaintiffs Nancy and William Infield believed that Quest would protect their Personal Information once they provided it to Quest.

69. Plaintiffs Nancy and William Infield would not have provided Quest with their Personal Information nor used Quest to provide blood testing had they known that it would fail to protect their Personal Information.

70. Plaintiffs Nancy and William Infield suffered and will continue to suffer damages due to the Data Breach.

C. Plaintiff Annie Mae Smith

71. Plaintiff Annie Mae Smith is a citizen and resident of Florida.

72. Plaintiff Smith was a Quest patient who went to a Quest laboratory to obtain blood testing services.

73. Plaintiff Smith provided Quest with her Personal Information as part of obtaining blood testing.

74. Plaintiff Smith's bill from Quest was subsequently sent to AMCA.

75. Plaintiff Smith received from AMCA notifications of the data breach dated June 4, 2019 and June 6, 2019.

76. AMCA informed Plaintiff Smith that information including her first and last name, her Social Security Number, the name of her lab or medical service provider, the date of her medical service, her referring doctor and other medical information may have been stored on AMCA's system that was compromised.

77. As a Quest patient, Plaintiff Smith believed that Quest would protect her Personal Information once she provided it to Quest.

78. Plaintiff Smith would not have provided Quest with her Personal Information nor used Quest to provide blood testing had she known that it would fail to protect her Personal Information.

79. Plaintiff Smith suffered and will continue to suffer damages due to the Data Breach.

V. INDIANA

A. Plaintiff Shannon Walden

80. Plaintiff Shannon Walden is a citizen and resident of Indiana

81. Plaintiff Walden was a Quest patient who went to a Quest laboratory to obtain blood testing services in or about May 2018.

82. Plaintiff Walden provided Quest with her Personal Information as part of obtaining blood testing.

83. Plaintiff Walden's unpaid bill from Quest was subsequently sent to AMCA.

84. Plaintiff Walden received a notice of data breach from Quest Diagnostics and Optum 360 dated July 8, 2019 informing her that her Personal Information was compromised in the Data Breach. The letter informed her that the information at risk included her "information used to identify and contact you (such as first, middle and last name, date of birth, address, phone number); information related to your providers and the services (such as dates of service, name of lab, referring doctor, test names, internal patient identification number); and laboratory billing- and payment-related information (such as insurance/payer information and identification number, diagnosis codes, internal account number)."

85. In response to the Data Breach, Plaintiff Walden took measures to protect herself, including spending 5 hours monitoring her financial accounts and credit score for fraudulent activity. Plaintiff Walden is continuing to investigate potentially fraudulent activity in a new financial account and expects to spend additional time investigating this activity.

86. Plaintiff Walden has experienced significant stress and anxiety from the Data Breach.

87. As a Quest patient, Plaintiff Walden believed that Quest would protect her Personal Information once she provided it to Quest.

88. Plaintiff Walden would not have provided Quest with her Personal Information nor used Quest for testing had she known that it would fail to protect her Personal Information.

89. Plaintiff Walden suffered and will continue to suffer damages due to the Data Breach.

90. In response to the Data Breach, Plaintiff Walden took measures to protect herself, including spending 5 hours monitoring her financial accounts and credit score for fraudulent activity. Plaintiff Walden is continuing to investigate potentially fraudulent activity in a new financial account and expects to spend additional time investigating this activity.

91. As a Quest patient, Plaintiff Walden believed that Quest would protect her Personal Information once she provided it to Quest.

92. Plaintiff Walden would not have provided Quest with her Personal Information nor used Quest for testing had she known that it would fail to protect her Personal Information.

93. Plaintiff Walden suffered and will continue to suffer damages due to the Data Breach.

VI. IOWA

A. Plaintiff Lucinda Dirks

94. Plaintiff Lucinda Dirks is a citizen and resident of Iowa.

95. Plaintiff Dirks was a Quest patient who went to a Quest laboratory to obtain blood testing services.

96. Plaintiff Dirks provided Quest with her Personal Information as part of obtaining blood testing.

97. Plaintiff Dirks's bill from Quest was subsequently sent to AMCA.

98. AMCA notified Plaintiff Dirks via letter on June 4, 2019, of the Data Breach.

99. AMCA informed Plaintiff Dirks that information including her first and last name, her Social Security Number, the name of her lab or medical service provider, the date of her medical service, her referring doctor and other medical information may have been stored on AMCA's system that was compromised.

100. In response to the Data Breach, Plaintiff Dirks has spent 40 hours monitoring her credit and financial accounts for fraudulent activity.

101. As a Quest patient, Plaintiff Dirks believed that Quest would protect her Personal Information once she provided it to Quest.

102. Plaintiff Dirks would not have provided Quest with her Personal Information nor used Quest to provide blood testing had she known that it would fail to protect her Personal Information.

103. Plaintiff Dirks suffered and will continue to suffer damages due to the Data Breach.

VII. KANSAS

A. Plaintiff Ashley Finch

104. Plaintiff Ashley Finch is a citizen and resident of Kansas.

105. Plaintiff Finch has a chronic medical condition that requires quarterly diagnostic tests.

106. Plaintiff Finch was a Quest patient who went to a Quest laboratory to obtain blood testing services.

107. Plaintiff Finch has used Quest regularly since 2016.

108. Plaintiff Finch reviewed and agreed to Quest's privacy policies on an iPad prior to agreeing to obtain blood testing services.

109. Plaintiff Finch provided Quest with her Personal Information as part of obtaining blood testing.

110. Plaintiff Finch's bill from Quest was subsequently sent to AMCA.

111. Pursuant to a January 1, 2018 letter, AMCA sought to collect $108.24 from Plaintiff Finch on behalf of Quest.

112. AMCA notified Plaintiff Finch of the Data Breach in a letter dated June 4, 2019.

113. AMCA informed Plaintiff Finch that information including her first and last name, her Social Security Number, the name of her lab or medical service provider, the date of her medical service, her referring doctor and other medical information may have been stored on AMCA's system that was compromised.

114. As a result of the Data Breach, Plaintiff Finch spends 10-20 minutes per week checking her credit report through Experian and Credit Karma.

115. As a Quest patient, Plaintiff Finch believed that Quest would protect her Personal Information once she provided it to Quest.

116. Plaintiff Finch would not have provided Quest with her Personal Information nor used Quest to provide blood testing had she known that it would fail to protect her Personal Information.

117. Plaintiff Finch suffered and will continue to suffer damages due to the Data Breach.

VIII. KENTUCKY

A. Plaintiff Carolyn Green

118. Plaintiff Carolyn Green is a citizen and resident of Kentucky.

119. Plaintiff Green was a Quest patient who went to a Quest laboratory to obtain blood testing services.

120. Plaintiff Green provided Quest with her Personal Information as part of obtaining blood testing.

121. Plaintiff Green's bill from Quest was subsequently sent to AMCA.

122. AMCA notified Plaintiff Green via letter on June 4, 2019, of the Data Breach.

123. AMCA informed Plaintiff Green that information including her first and last name, her Social Security Number, the name of her lab or medical service provider, the date of her medical service, her referring doctor and other medical information may have been stored on AMCA's system that was compromised.

124. As a Quest patient, Plaintiff Green believed that Quest would protect her Personal Information once she provided it to Quest.

125. Plaintiff Green would not have provided Quest with her Personal Information nor used Quest to provide blood testing had she known that it would fail to protect her Personal Information.

126. Plaintiff Green suffered and will continue to suffer damages due to the Data Breach.

B. Plaintiff Rose Marie Perry

127. Plaintiff Rose Marie Perry is a citizen and resident of Kentucky.

128. Plaintiff Perry was a Quest patient who went to a Quest laboratory to obtain blood testing services.

129. Plaintiff Perry provided Quest with her Personal Information as part of obtaining blood testing.

130. Plaintiff Perry's bill from Quest was subsequently sent to Defendants' billing collections vendor, AMCA.

131. Plaintiff Perry received a notice of data breach from Quest Diagnostics and Optum 360 dated July 8, 2019.

132. Plaintiff Perry's letter from Quest and Optum360 dated informed her that her Personal Information was compromised in the Data Breach. It noted that the information at risk included her "information used to identify and contact you (such as first, middle and last name,

date of birth, address, phone number); information related to your providers and the services (such as dates of service, name of lab, referring doctor, test names, internal patient identification number); and laboratory billing- and payment-related information (such as insurance/payer information and identification number, diagnosis codes, internal account number)."

133. In response to the Data Breach, Plaintiff Perry took mitigative measures, including spending substantial time monitoring her accounts for fraudulent activity.

134. As a Quest patient, Plaintiff Perry believed that Quest would protect her Personal Information once she provided it to Quest.

135. Plaintiff Perry would not have provided Quest with her Personal Information nor used Quest to provide blood testing had she known that it would fail to protect her Personal Information.

136. Plaintiff Perry suffered and will continue to suffer damages due to the Data Breach.

IX. MICHIGAN

A. Plaintiff Michael Rutan

137. Plaintiff Michael Rutan is a citizen and resident of Michigan.

138. Plaintiff Rutan was a Quest patient whose blood samples were sent to a Quest laboratory on multiple occasions within the past several years.

139. Plaintiff Rutan provided Quest with his Personal Information as part of obtaining blood testing services.

140. Plaintiff Rutan's bill from Quest was subsequently sent to AMCA.

141. Plaintiff Rutan received a letter from Quest and Optum360 dated July 8, 2019 informing him that his Personal Information was compromised in the Data Breach. It noted that the information at risk included his "information used to identify and contact you (such as first, middle and last name, date of birth, address, phone number); information related to your

providers and the services (such as dates of service, name of lab, referring doctor, test names, internal patient identification number); and laboratory billing- and payment-related information (such as insurance/payer information and identification number, diagnosis codes, internal account number)."

142. Within the past year, after the Data Breach began, Plaintiff Rutan started receiving more frequent mailings for pre-approved credit cards, and an increased volume of robocalls.

143. In response to the Data Breach, Plaintiff Rutan took mitigative measures, including spending substantial time monitoring his accounts for fraudulent activity.

144. As a Quest patient, Plaintiff Rutan believed that Quest would protect his Personal Information once it was provided to Quest.

145. Plaintiff Rutan would not have provided Quest with this Personal Information nor used Quest to provide blood testing had he known that it would fail to protect his Personal Information.

146. Plaintiff Rutan suffered and will continue to suffer damages due to the Data Breach.

X. MINNESOTA

A. Plaintiff Elizabeth Hollway

147. Plaintiff Elizabeth Hollway is a citizen and resident of Minnesota.

148. Plaintiff Hollway was a Quest patient who went to a Quest laboratory to obtain blood testing services on, among other dates, May 8, 2018, June 22, 2018, and August 1, 2018.

149. Plaintiff Hollway reviewed and agreed to Quest's privacy policies on an iPad prior to agreeing to obtain blood testing services.

150. Plaintiff Hollway provided Quest with her Personal Information as part of obtaining blood testing.

151. Plaintiff Hollway's bill from Quest was subsequently sent to AMCA.

152. Plaintiff Hollway paid Quest for the testing services on August 1, 2018.

153. Plaintiff Hollway paid AMCA for Quest's services on January 8, 2019.

154. AMCA notified Plaintiff Hollway via letter on June 4, 2019 of the Data Breach.

155. In that letter, AMCA informed Plaintiff Hollway that information including her first and last name, her Social Security Number, the name of her lab or medical service provider, the date of her medical service, her referring doctor and other medical information may have been stored on AMCA's system that was compromised.

156. As a result of the data breach, on June 10, 2019 Plaintiff Hollway experienced unauthorized charges on her credit card.

157. On June 10, 2019, an unauthorized individual purchased a $200 restaurant gift card using Plaintiff Hollway's Personal Information.

158. Plaintiff Hollway also experienced identify theft: an unauthorized individual opened a Nordstrom credit card in her name as a result of the data breach.

159. Plaintiff Hollway was informed that whoever opened the Nordstrom account provided Nordstrom with her name, Social Security number, and date of birth.

160. To attempt to resolve the identity theft issues caused by the Data Breach, Plaintiff Hollway spent 15 hours contacting Transunion, Equifax, Experian, her mortgage companies and banks where she held accounts, credit cards, and debit cards.

161. Additionally to attempt to resolve the issues, Plaintiff Hollway purchased a monthly subscription to Lifelock for identity theft protection for $31.96 per month.

162. As a Quest patient, Plaintiff Hollway believed that Quest would protect her Personal Information once she provided it to Quest.

163. Plaintiff Hollway would not have provided Quest with her Personal Information nor used Quest to provide blood testing had she known that it would fail to protect her Personal Information.

164. Plaintiff Hollway suffered and will continue to suffer damages due to the Data Breach.

XI. MISSOURI

A. Plaintiff LaTease Rikard

165. Plaintiff LaTease Rikard is a citizen and resident of Missouri.

166. Plaintiff Rikard was a Quest patient who went to a Quest laboratory to obtain blood testing services several times in the past few years.

167. Plaintiff Rikard provided Quest with her Personal Information as part of obtaining blood testing.

168. Plaintiff Rikard's bill from Quest was subsequently sent to AMCA.

169. Plaintiff Rikard received a letter from Quest and Optum360 dated July 8, 2019 informing her that her Personal Information was compromised in the Data Breach. It noted that the information at risk included her "information used to identify and contact you (such as first, middle and last name, date of birth, address, phone number); information related to your providers and the services (such as dates of service, name of lab, referring doctor, test names, internal patient identification number); and laboratory billing- and payment-related information (such as insurance/payer information and identification number, diagnosis codes, internal account number)."

170. In response to the Data Breach, Plaintiff Rikard took mitigative measures, including spending substantial time monitoring her accounts for fraudulent activity.

171. As a Quest patient, Plaintiff Rikard believed that Quest would protect her Personal Information once she provided it to Quest.

172. Plaintiff Rikard would not have provided Quest with her Personal Information nor used Quest to provide blood testing had she known that Quest would fail to protect her Personal Information.

173. Plaintiff Rikard suffered and will continue to suffer damages due to the Data Breach.

XII. NEW HAMPSHIRE

A. Plaintiff Naomi Jaworowski

174. Plaintiff Naomi Jaworowski is a citizen and resident of New Hampshire.

175. Plaintiff Jaworowski was a Quest patient who went to a Quest laboratory to obtain blood testing services approximately two years ago.

176. Plaintiff Jaworowski provided Quest with her Personal Information as part of obtaining blood testing.

177. Plaintiff Jaworowski's bill from Quest was subsequently sent to AMCA.

178. Plaintiff Jaworowski received a letter from Quest and Optum360 dated July 8, 2019 informing her that her Personal Information was compromised in the Data Breach. It noted that the information at risk included her "information used to identify and contact you (such as first, middle and last name, date of birth, address, phone number); information related to your providers and the services (such as dates of service, name of lab, referring doctor, test names, internal patient identification number); and laboratory billing- and payment-related information (such as insurance/payer information and identification number, diagnosis codes, internal account number)."

179. In response to the Data Breach, Plaintiff Jaworowski called the Attorney General's Office to ask how she can protect herself. She also called Quest for more information about the breach. She also took mitigative measures, including spending substantial time monitoring her accounts for fraudulent activity.

180. As a Quest patient, Plaintiff Jaworowski believed that Quest would protect her Personal Information once she provided it to Quest.

181. Plaintiff Jaworowski would not have provided Quest with her Personal Information nor used Quest to provide blood testing had she known that Quest would fail to protect her Personal Information.

182. Plaintiff Jaworowski suffered and will continue to suffer damages due to the Data Breach.

XIII. NEW JERSEY

A. Plaintiff Ria Jairam

183. Plaintiff Ria Jairam is a citizen and resident of New Jersey.

184. Plaintiff Jairam was a Quest patient who went to a Quest laboratory to obtain blood testing services.

185. Plaintiff Jairam provided Quest with her Personal Information as part of obtaining blood testing.

186. Plaintiff Jairam's bill from Quest was subsequently sent to Defendants' billing collections vendor, AMCA.

187. Plaintiff Jairam received a letter from Quest and Optum360 dated July 8, 2019 informing her that her Personal Information was compromised in the Data Breach. It noted that the information at risk included her "information used to identify and contact you (such as first, middle and last name, date of birth, address, phone number); information related to your providers

and the services (such as dates of service, name of lab, referring doctor, test names, internal patient identification number); and laboratory billing- and payment-related information (such as insurance/payer information and identification number, diagnosis codes, internal account number)."

188. Plaintiff Jairam suffered identify theft as a result of the Data Breach.

189. Following the Data Breach, Plaintiff Jairam's Chase Bank account was compromised and $2,000 was fraudulently withdrawn. As a result, Plaintiff Jairam had to close her bank accounts and cancel her credit cards.

190. Plaintiff Jairam was informed by Navy Federal Credit Union of additional possible fraudulent activity requiring new bank accounts to be opened.

191. To attempt to resolve the identity theft issues caused by the Data Breach, Plaintiff Jairam spent 12 hours reviewing her bank accounts as a result of these fraudulent activities.

192. As a Quest patient, Plaintiff Jairam believed that Quest would protect her Personal Information once she provided it to Quest.

193. Plaintiff Jairam would not have provided Quest with her Personal Information nor used Quest to provide blood testing had she known that it would fail to protect her Personal Information.

194. Plaintiff Jairam suffered and will continue to suffer damages due to the Data Breach.

B. Plaintiff Cynthia Connor

195. Plaintiff Cynthia Connor is a citizen and resident of New Jersey.

196. Plaintiff Connor was a Quest patient who went to a Quest laboratory to obtain a biopsy on January 9, 2018.

197. Plaintiff Connor provided Quest with her Personal Information as part of obtaining its services.

198. Plaintiff Connor's bill from Quest was subsequently sent to AMCA.

199. On December 3, 2018, Plaintiff Connor received a collection bill for $130.87 from AMCA regarding the services provided by Quest Diagnostics Inc.

200. Plaintiff Connor paid her bill through AMCA's website.

201. As a Quest patient, Plaintiff Connor believed that Quest would protect her Personal Information once she provided it to Quest.

202. Plaintiff Connor would not have provided Quest with her Personal Information nor used Quest to provide services had she known that it would fail to protect her Personal Information.

203. Plaintiff Connor suffered and will continue to suffer damages due to the Data Breach.

XIV. NEW YORK

A. Plaintiff John Briley

204. Plaintiff John Briley is a citizen and resident of New York.

205. Plaintiff Briley was a Quest patient who went to a Quest laboratory to obtain blood testing in at least the past two to three years.

206. Plaintiff Briley provided Quest with his Personal Information as part of obtaining blood testing.

207. Plaintiff Briley's bill from Quest was subsequently sent to AMCA.

208. Plaintiff Briley received a letter from Quest and Optum360 dated July 8, 2019 informing him that his Personal Information was compromised in the Data Breach. It noted that the information at risk included his "information used to identify and contact you (such as first, middle and last name, date of birth, address, phone number); information related to your providers

and the services (such as dates of service, name of lab, referring doctor, test names, internal patient identification number); and laboratory billing- and payment-related information (such as insurance/payer information and identification number, diagnosis codes, internal account number)."

209. His eighteen year old daughter received a similar letter from Quest dated July 8, 2019 regarding blood testing services she obtained under his insurance plan.

210. Plaintiff Briley received a letter from TD Bank dated October 2, 2019 regarding a fraudulent "application for an account with Samsung Financing." An imposter attempted to open the account using a false name and Plaintiff Briley's mailing address. The application was denied.

211. Plaintiff Briley had not experienced any similar fraudulent activity prior to the Quest data breach.

212. In response to the Data Breach, Plaintiff Briley took mitigative measures, including spending substantial time monitoring his accounts for fraudulent activity.

213. As a Quest patient, Plaintiff Briley believed that Quest would protect his Personal Information once he provided it to Quest.

214. Plaintiff Briley would not have provided Quest with this Personal Information nor used Quest to provide blood testing had he known that it would fail to protect his Personal Information.

215. Plaintiff Briley suffered and will continue to suffer damages due to the Data Breach.

B. Plaintiff Karli Parker

216. Plaintiff Karli Parker is a citizen and resident of New York.

217. Plaintiff Parker was a Quest patient who went to a Quest laboratory to obtain blood testing services approximately two years ago.

218. Plaintiff Parker provided Quest with her Personal Information as part of obtaining blood testing.

219. Plaintiff Parker's bill from Quest was subsequently sent to AMCA.

220. Plaintiff Parker received a letter from Quest and Optum360 dated July 8, 2019 informing her that her Personal Information was compromised in the Data Breach. It noted that the information at risk included her "information used to identify and contact you (such as first, middle and last name, date of birth, address, phone number); information related to your providers and the services (such as dates of service, name of lab, referring doctor, test names, internal patient identification number); and laboratory billing- and payment-related information (such as insurance/payer information and identification number, diagnosis codes, internal account number)."

221. In response to the Data Breach, Plaintiff Parker took mitigative measures, including spending substantial time monitoring her accounts for fraudulent activity.

222. As a Quest patient, Plaintiff Parker believed that Quest would protect her Personal Information once she provided it to Quest.

223. Plaintiff Parker would not have provided Quest with her Personal Information nor used Quest to provide blood testing had she known that Quest would fail to protect her Personal Information.

224. Plaintiff Parker suffered and will continue to suffer damages due to the Data Breach.

C. Plaintiff Joyce Rosselli

225. Plaintiff Joyce Rosselli is a citizen and resident of New York.

226. Plaintiff Rosselli was a Quest patient who went to a Quest laboratory to obtain blood testing services several times over the last few years.

227. Plaintiff Rosselli provided Quest with her Personal Information as part of obtaining blood testing.

228. Plaintiff Rosselli's bill from Quest was subsequently sent to AMCA.

229. On June 4, 2019, Plaintiff Rosselli received a letter from AMCA informing her that her Personal Information including her "first and last name, Social Security number, name of lab or medical service provider, date of medical service, referring doctor, [and] certain other medical information" was at risk due to the Data Breach.

230. In response to the Data Breach, Plaintiff Rosselli signed up for the free two-year credit monitoring service offered by AMCA.

231. In further response to the Data Breach, on June 17, 2019, Plaintiff Rosselli placed a "fraud alert" on her credit report.

232. In response to the Data Breach, Plaintiff Rosselli took mitigative measures, including spending substantial time monitoring her accounts for fraudulent activity.

233. Plaintiff Rosselli received an alert from her Capital One CreditWise fraud monitoring product stating that her email address was found on the "dark web" on June 8, 2019 and July 6, 2019. Those dates were several months after hackers first accessed AMCA's system.

234. On or around July 11, 2019, Plaintiff Rosselli called Quest's data breach hotline to determine whether her involvement in the Data Breach was related to Quest. The Quest representative confirmed that her involvement in the breach was in fact related to Quest.

235. As a Quest patient, Plaintiff Rosselli believed that Quest would protect her Personal Information once she provided it to Quest.

236. Plaintiff Rosselli would not have provided Quest with her Personal Information nor used Quest to provide blood testing had she known that it would fail to protect her Personal Information.

237. Plaintiff Rosselli suffered and will continue to suffer damages due to the Data Breach.

XV. OHIO

A. Plaintiff Deanna Taylor

238. Plaintiff Deanna Taylor is a citizen and resident of Ohio.

239. Plaintiff Taylor was a Quest patient who obtained blood testing through Quest within the past two years.

240. Plaintiff Taylor provided Quest with her Personal Information as part of obtaining blood testing.

241. Plaintiff Taylor's bill from Quest was subsequently sent to AMCA.

242. In November 2019, Plaintiff Taylor called Quest's data breach hotline to verify that she was involved in the Data Breach. The Quest representative confirmed that she was in fact involved in the Data Breach.

243. In response to the Data Breach, Plaintiff Taylor took mitigative measures, including spending substantial time monitoring her accounts for fraudulent activity.

244. As a Quest patient, Plaintiff Taylor believed that Quest would protect her Personal Information once she provided it to Quest.

245. Plaintiff Taylor would not have provided Quest with this Personal Information nor used Quest to provide blood testing had she known that it would fail to protect her Personal Information.

246. Plaintiff Taylor suffered and will continue to suffer damages due to the Data Breach.

XVI. PENNSYLVANIA

A. Plaintiff William Lindsay

247. Plaintiff William Lindsay is a citizen and resident of Pennsylvania.

248. Plaintiff Lindsay was a Quest patient who went to a Quest laboratory to obtain blood and urine testing services.

249. Beginning in 2014, Plaintiff Lindsay used Quest Diagnostics on a regular basis. Over the last two years, he used Quest's services every other month.

250. Plaintiff Lindsay provided Quest with his Personal Information as part of obtaining blood testing.

251. Due to a disputed charge, Plaintiff Lindsay's bill from Quest was subsequently sent to Defendants' billing collections vendor, AMCA.

252. AMCA notified Plaintiff Lindsay by letter dated June 4, 2019, of the Data Breach.

253. AMCA informed Plaintiff Lindsay that information including his first and last name, his Social Security Number, the name of his lab or medical service provider, the date of his medical service, his referring doctor and other medical information may have been stored on AMCA's system that was compromised.

254. As a result of the Data Breach, Plaintiff Lindsay had to get new debit cards.

255. As a result of the Data Breach, Plaintiff Lindsay now spends one hour per week auditing his bank statements.

256. As a result of the Data Breach, Plaintiff Lindsay purchased Capital One Credit Monitoring.

257. As a Quest patient, Plaintiff Lindsay believed that Quest would protect his Personal Information once he provided it to Quest.

258. Plaintiff Lindsay would not have provided Quest with his Personal Information nor used Quest to provide blood testing had he known that it would fail to protect his Personal Information.

259. Plaintiff Lindsay suffered and will continue to suffer damages due to the Data Breach.

B. Plaintiff Brittney Petitta

260. Plaintiff Brittney Petitta is a citizen and resident of Pennsylvania.

261. Plaintiff Petitta was a Quest patient who went to a Quest laboratory to obtain blood testing services in at least 2018.

262. Plaintiff Petitta provided Quest with her Personal Information as part of obtaining blood testing.

263. Plaintiff Petitta's bill from Quest was subsequently sent to AMCA.

264. Plaintiff Petitta received a letter from Quest and Optum360 dated July 8, 2019 informing her that her Personal Information was compromised in the Data Breach. It noted that the information at risk included her "information used to identify and contact you (such as first, middle and last name, date of birth, address, phone number); information related to your providers and the services (such as dates of service, name of lab, referring doctor, test names, internal patient identification number); and laboratory billing- and payment-related information (such as insurance/payer information and identification number, diagnosis codes, internal account number)."

265. In response to the Data Breach, Plaintiff Petitta took mitigative measures, including spending substantial time monitoring her accounts for fraudulent activity.

266. As a Quest patient, Plaintiff Petitta believed that Quest would protect her Personal Information once she provided it to Quest.

267. Plaintiff Petitta would not have provided Quest with her Personal Information nor used Quest to provide blood testing had she known that Quest would fail to protect her Personal Information.

268. Plaintiff Petitta suffered and will continue to suffer damages due to the Data Breach.

C. Plaintiff Darlane Saracina

269. Plaintiff Darlane Saracina is a citizen and resident of Pennsylvania.

270. Plaintiff Saracina was a Quest patient who went to a Quest laboratory to obtain blood testing services several times over the last few years.

271. Plaintiff Saracina provided Quest with her Personal Information as part of obtaining blood testing.

272. Plaintiff Saracina's bill from Quest was subsequently sent to AMCA.

273. Plaintiff Saracina received a letter from Quest in or around July 2019 informing her that her Personal Information was at risk due to the Data Breach.

274. On October 10, 2019, Plaintiff Saracina also called the Quest data breach hotline to confirm that her involvement in the Data Breach was related to Quest. The Quest representative verified that her involvement in the breach was in fact related to Quest.

275. Plaintiff Saracina received an alert from her Capital One CreditWise fraud monitoring product stating that her Social Security number was found on the "dark web" on September 25, 2018. That date was nearly two months after hackers first accessed AMCA's system.

276. In response to the Data Breach, Plaintiff Saracina took mitigative measures, including spending substantial time monitoring her accounts and fraud monitoring service for fraudulent activity.

277. As a Quest patient, Plaintiff Saracina believed that Quest would protect her Personal Information once she provided it to Quest.

278. Plaintiff Saracina would not have provided Quest with her Personal Information nor used Quest to provide blood testing had she known that it would fail to protect her Personal Information.

279. Plaintiff Saracina suffered and will continue to suffer damages due to the Data Breach.

XVII. TENNESSEE

A. Plaintiff Jo Ann Buck

280. Plaintiff Jo Ann Buck is a citizen and resident of Tennessee.

281. Plaintiff Buck was a Quest patient who went to a Quest laboratory to obtain blood testing services within the past few years.

282. Plaintiff Buck provided Quest with her Personal Information as part of obtaining blood testing.

283. Plaintiff Buck's bill from Quest was subsequently sent to AMCA.

284. Plaintiff Buck received a letter from Quest and Optum360 dated July 8, 2019 informing her that her Personal Information was compromised in the Data Breach. It noted that the information at risk included her "information used to identify and contact you (such as first, middle and last name, date of birth, address, phone number); information related to your providers and the services (such as dates of service, name of lab, referring doctor, test names, internal patient identification number); and laboratory billing- and payment-related information (such as

insurance/payer information and identification number, diagnosis codes, internal account number)."

285. In response to the Data Breach, Plaintiff Buck took mitigative measures, including spending substantial time monitoring her accounts for fraudulent activity.

286. As a Quest patient, Plaintiff Buck believed that Quest would protect her Personal Information once she provided it to Quest.

287. Plaintiff Buck would not have provided Quest with her Personal Information nor used Quest to provide blood testing had she known that Quest would fail to protect her Personal Information.

288. Plaintiff Buck suffered and will continue to suffer damages due to the Data Breach.

XVIII. TEXAS

A. Plaintiff Ann Davis

289. Plaintiff Ann Davis is a citizen and resident of Texas.

290. Plaintiff Davis was a Quest patient who went to a Quest laboratory to obtain blood testing at least once per year for the past several years.

291. Plaintiff Davis provided Quest with her Personal Information as part of obtaining blood testing services.

292. Quest sent multiple bills of Plaintiff Davis to collections. At least one such bill was sent to AMCA.

293. Plaintiff Davis received a letter from AMCA dated June 4, 2019 informing her that her Personal Information including her "first and last name, Social Security Number, name of lab or medical service provider, date of medical service, referring doctor, [and] certain other medical information" was at risk due to the Data Breach.

294. In or around early 2019, Plaintiff Davis received a call from her credit card company stating that someone charged $800 for a fraudulent purchase at Boost Mobile. The credit card company issued her a replacement card. Plaintiff Davis believes the compromised card was the same card she used to pay Quest bills in the past.

295. In response to the Data Breach, Plaintiff Davis took mitigative measures, including spending substantial time monitoring her accounts for fraudulent activity. She spends one to two hours per week checking her accounts. She also spent approximately two hours in connection with the credit card fraud.

296. Plaintiff Davis also purchased a new antivirus product due at least in part to her fear of harm from the Data Breach.

297. As a Quest patient, Plaintiff Davis believed that Quest would protect her Personal Information once she provided it to Quest.

298. Plaintiff Davis would not have provided Quest with this Personal Information nor used Quest to provide blood testing had she known that it would fail to protect her Personal Information.

299. Plaintiff Davis suffered and will continue to suffer damages due to the Data Breach.

DEFENDANTS

300. Quest Diagnostics Incorporated is a Delaware corporation with its principal place of business in Secaucus, New Jersey.

301. Optum360, LLC is a Delaware limited liability company with its principal place of business in Eden Prairie, Minnesota.

FACTUAL ALLEGATIONS

A. Quest Collects Patients' Personal Information And Shares It With Optum360 and AMCA

302. Quest markets itself as "the world's leading provider of diagnostic information services." Quest's operations are national in scope and the company purports to annually serve one in three adult Americans and half the physicians and hospitals in the United States. Quest generated revenues of approximately $7.53 billion in 2018.

303. Quest's business operations include operating over 2,200 "Patient Service Centers" where patient's blood is drawn and tested following an order from a doctor.[1] These blood tests relate to a wide array of medical conditions, including but not limited to: allergy and asthma, human immunodeficiency virus (HIV), ovarian, breast and other cancer screening, hepatitis C, and prenatal health screening.

304. Quest states that it "obtains diagnosis information from the ordering physicians [sic] office."[2] Quest also asks its patients to bring photo identification, current health insurance information, and permits alternative methods of payment for costs in excess or beyond the scope of the patient's insurance and if the patient is uninsured.[3]

305. Quest's invoices cover laboratory testing fees only and are separate from any bill received by a patient's physician. Patients can be charged following an in-person visit to a Quest

---

[1] https://questdiagnostics.com/home/patients/preparing-for-test/get-started (last visited September 27, 2019).

[2] Quest Diagnostics, Frequently Asked Questions: Billing Services, "Where does Quest Diagnostics obtain the diagnosis information related to my claim?" https://billing.questdiagnostics.com/PatientBilling/PATFaqExternal.action?getLabCode=false&fromLink=doFaq (last visited September 27, 2019).

[3] https://questdiagnostics.com/home/patients/preparing-for-test/get-started (last visited September 27, 2019).

Patient Service Center or when their physician sends their specimen to a Quest Diagnostics laboratory.[4] Patients are responsible for paying Quest for performing diagnostic services either through their insurance or out-of-pocket where the patient does not have insurance or the costs are not covered in whole or part.

306. If Quest's patients fail to pay their invoices within the requested time period, Quest employs an associated business for collection. Prior to September 2016, Quest's collection agent by contract or direct association was AMCA. In September 2016, Quest partnered with Optum360 so that Quest's revenue services operations would become part of Optum360.[5] Thereafter, Quest assigned its contract with AMCA to Optum360 and AMCA delivered Quest's outstanding invoices, including Quest patients' Personal Information, to AMCA.[6] Before and after Quest assigned its contract to Optum360, Quest provided its patients' Personal Information directly to AMCA.

307. Upon information and belief, in order to facilitate collection, Quest and/or Optum360 would provide AMCA with Quest patients' Personal Information which AMCA subsequently stored in its own computer systems. It is unclear why Defendants would provide extremely sensitive health and diagnostic information to a collection agent who is solely responsible for bill collection.

---

[4] Quest Diagnostics, Frequently Asked Questions: Billing Services, "Why have I received an invoice from Quest Diagnostics?" https://billing.questdiagnostics.com/PatientBilling/PATFaqExternal.action?getLabCode=false&fromLink=doFaq (last visited September 27, 2019).

[5] Optum and Quest Diagnostics Partner to Help Make the Health System Work Better for Patients, Physicians, Health Plans and Employers, Sept. 13, 2016, https://www.optum.com/about/news/optum-quest-diagnostics-partner-help-make-health-system-work-better-for-patients-physicians-health-plans-employers.html (last visited September 27, 2019).

[6] Quest Diagnostics Incorporated, 2018 Annual Report (Form 10-K), at 58.

308. In U.S. Bankruptcy Court in the Southern District of New York, AMCA has admitted that its "business, by its very nature, requires it to collect and maintain data transmitted to it by its clients [such as Quest] that includes personally identifiable information about third-party debtors that could include names, home addresses, social security numbers, bank account information for consumers choosing to pay online by check and, for consumers choosing to pay their outstanding balances by credit card, credit card information." AMCA has also admitted that this "information might also include dates of birth and certain medical information related to any laboratory tests for which payment is sought."[7]

309. In addition, as part of AMCA's billing collection services for Defendants, Plaintiffs furnished Personal Information to AMCA, which AMCA subsequently stored.

B. The Data Breach

310. On June 3, 2019, Quest publicly announced the following in a filing with the SEC:

> On May 14, 2019, American Medical Collection Agency (AMCA), a billing collections vendor, notified Quest Diagnostics Incorporated ("Quest Diagnostics") and Optum360 LLC, Quest Diagnostics' revenue cycle management provider, of potential unauthorized activity on AMCA's web payment page. Quest Diagnostics and Optum360 promptly sought information from AMCA about the incident, including what, if any, information was subject to unauthorized access.
>
> Although Quest Diagnostics and Optum360 have not yet received detailed or complete information from AMCA about the incident, AMCA has informed Quest Diagnostics and Optum360 that:
>
> - between August 1, 2018 and March 30, 2019 an unauthorized user had access to AMCA's system that contained information that AMCA had received from various entities, including Quest Diagnostics, and information that AMCA collected itself;
> - the information on AMCA's affected system included financial information (*e.g.*, credit card numbers and bank account information), medical information and other personal information (*e.g.*, Social Security Numbers);

[7] Declaration of Russell H. Fuchs Pursuant to Local Bankruptcy Rule 1007-2 and in Support of "First Day" Motions, *In re Retrieval-Masters Creditors Bureau, Inc.*, No. 19-23185-RDD (Bankr. S.D.N.Y. June 17, 2019), ECF No. 2 at 4-5.

- as of May 31, 2019, AMCA believes that the number of Quest Diagnostics patients whose information was contained on AMCA's affected system was approximately 11.9 million people; and
- AMCA has been in contact with law enforcement regarding the incident.[8]

311. In a written statement attributed to AMCA, AMCA announced it is still investigating the breach:

> We are investigating a data incident involving an unauthorized user accessing the American Medical Collection Agency system. Upon receiving information from a security compliance firm that works with credit card companies of a possible security compromise, we conducted an internal review, and then took down our web payments page. . . . .We hired a third-party external forensics firm to investigate any potential security breach in our systems, migrated our web payments portal services to a third-party vendor, and retained additional experts to advise on, and implement, steps to increase our systems' security. We have also advised law enforcement of this incident. We remain committed to our system's security, data privacy, and the protection of personal information.

312. Although Quest reported that it had only learned of the Data Breach from AMCA on May 14, 2019, the breach was actually discovered at least three months prior to Quest's SEC filing. At the end of February 2019, Gemini Advisory, a New York-based company that works with financial institutions to monitor the sale of consumer information on underground markets, identified a large number of compromised AMCA patient information for sale on the dark web.[9] As reported on May 10, 2019 by DataBreaches.net:

> On February 28, 2019, Gemini Advisory identified a large number of compromised payment cards while monitoring dark web marketplaces. Almost 15% of these records included additional personally identifiable information (PII), such as dates of birth (DOBs), Social Security numbers (SSNs), and physical addresses. A thorough analysis indicated that the information was likely stolen from the online portal of the American Medical Collection Agency (AMCA), one of the largest recovery agencies for patient collections. Several financial institutions also

[8] Quest Diagnostics Form 8-K, filed June 3, 2019, available at https://www.sec.gov/Archives/edgar/data/1022079/000094787119000415/ss138857_8k.htm (last visited June 18, 2019).

[9] Gemini Advisory, *AMCA Breach May be Largest Medical Breach in 2019* (June 4, 2019), available at https://geminiadvisory.io/amca-largest-medical-breach/ (last visited June 18, 2019).

collaboratively confirmed the connection between the compromised payment card data and the breach at AMCA.[10]

313. Gemini's additional research revealed AMCA's exposure window had lasted for at least seven months beginning in September 2018.[11]

314. On March 1, 2019, Gemini Advisory attempted to notify AMCA of the data exposure but received no response. Gemini Advisory then contacted federal law enforcement who reportedly followed-up with AMCA.[12]

315. Following notification from law enforcement, AMCA's payment portal became unavailable for weeks.[13]

316. In its notice to patients affected by the breach, AMCA claims it learned of the unauthorized access on March 20, 2019. Yet Quest failed to take any steps to notify patients whose information was affected until months later, initially only doing so generally through an SEC filing.

317. Subsequent to Quest's SEC filing, AMCA began sending out notices to those affected by the Data Breach. Quest stated on its website that it had "been advised by AMCA that

---

[10] Databreaches.net, *American Medical Collection Agency breach impacted 200,000 patients – Gemini Advisory* (posted May 10, 2019), available at https://www.databreaches.net/american-medical-collection-agency-breach-impacted-200000-patients-gemini-advisory/ (last visited June 18, 2019).

[11] *Id.*

[12] *Id.*

[13] *Id.*

if your social security number or financial information was involved in the incident, you will be notified by letter from AMCA[.]"[14]

318. On June 17, 2019, AMCA filed for Chapter 11 bankruptcy in the Southern District of New York stating an intention to liquidate. The bankruptcy filings describe the types of personal information maintained by AMCA, as well as additional specifics regarding the Data Breach. According to an affidavit submitted by Russell H. Fuchs, the Chief Executive Officer of AMCA:

> [AMCA] by its very nature, requires it to collect and maintain data transmitted to it by its clients that includes personally identifiable information about third-party debtors that could include names, home addresses, social security numbers, bank account information for consumers choosing to pay online by check and, for consumers choosing to pay their outstanding balances by credit card, credit card information. In the case of the AMCA business, that information might also include dates of birth and certain medical information related to any laboratory tests for which payment is sought. In all, at any given time, [AMCA] would have held tens of millions of individual points of data regarding millions of individual persons, none of which could be handled without a robust IT system.
>
> [AMCA]'s original IT architecture was built around an IBM mainframe-based system that ran on COBOL4 and served the [AMCA]'s purposes well for many years. However, with ever-increasing market demands for enhanced interconnectivity between the [AMCA]'s and its clients' systems, as well as for web-based interaction with both the [AMCA]'s clients and its clients' consumer and patient-debtors, it was clear that continued reliance on the [AMCA]'s internet-unconnected mainframe system would not be tenable in the long term.
>
> Accordingly, in 2015, after several years of internal planning and development, the [AMCA] began to transition to a proprietary, server-based, network-connected system. [AMCA] invested over a million dollars in the new system, employing outside IT consultants to ensure that the system would reflect current technological standards, including, importantly, appropriate data security protocols.[15]

---

[14] Quest Diagnostics, *AMCA Data Security Incident*, available at https://www.questdiagnostics.com/home/AMCA-data-breach-patients.html (last visited June 18, 2019).

[15] *In re Retrieval-Masters Creditors Bureau, Inc.*, No. 7:19-bk-23185, Dkt. Entry 2 (Bankr. S.D.N.Y. Jun 17, 2019).

319. Despite touting its investment in data security, AMCA acknowledged that it "first learned that there might be a problem" when it received a series of common point of purchase notifications that "suggested that a disproportionate number of credit cards that at some point had interacted with the [AMCA's] web portal were later associated with fraudulent charges."[16]

320. In response, AMCA "shut down its web portal to prevent any further compromises of customer data, and engaged outside consultants who were able to confirm that, in fact, [AMCA]'s servers … had been hacked as early as August, 2018." AMCA went on to explain that "the breach required [AMCA] to hire IT professionals and consultants from three different firms, to identify the source of the breach, diagnose its cause, and implement appropriate solutions. To date, these expenses alone cost approximately $400,000, and have effectively shut down outside entry into [AMCA]'s IT network by severely restricting access via the employment of individual authentication mechanisms, VPN access, or specifically vetted 'whitelists' of pre-approved IP's."[17]

321. AMCA stated that the costs of providing notice to affected individuals, coupled with the loss of its largest clients LabCorp and Quest, required it to reduce its workforce from 113 employees at year-end 2018 to just 25 employees as of June 17, 2019. As a result, AMCA stated it is "no longer is optimistic that it will be able to rehabilitate its business."[18]

322. Quest and Optum360 had a non-delegable duty to ensure that its systems and those of its vendors and business associates, including AMCA, were sufficient to adequately secure patient information. This was especially true after AMCA transitioned to a "network-connected"

---

16 *Id*.

17 *Id*.

18 *Id*.

system that included "enhanced interconnectivity" and "web-based interaction" between its systems and those of its clients such as Quest and Optum360.

323. By failing to adequately monitor and audit the data security systems of their vendors and business associates, Quest put patient information at severe risk. Following the news that Quest's customers were impacted by the Data Breach, several other labs, who are named as defendants in this action, also announced that their customers had been impacted by the Data Breach.

324. On July 1, 2019, Optum360 disclosed to the Department of Heath and Human Services' Office for Civil Rights that 11,500,000 individuals have been affected by the Data Breach.[19]

C. Defendants Failed To Exercise Due Care In Contracting With AMCA

325. Defendants failed to exercise reasonable care in protecting patients' information by contracting with AMCA to handle their debt collections.

326. AMCA's bankruptcy filings indicate it was thinly capitalized and had an insignificant information technology ("IT") department with little IT infrastructure. Public reporting has highlighted that AMCA was not a reputable business associate—let alone an associate to be trusted with Plaintiffs' and Class Members' Personal Information.

327. Specifically, AMCA's bankruptcy filings admit that it had less than $4 million in liquidity and its owner had to take a secured loan from his own personal funds simply to mail notices to those impacted by the Data Breach. Put simply, Quest should not have contracted with

[19] Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, U.S. Dep't of Health and Human Services, Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Nov. 11, 2019).

an entity that did not even have the means to mail notices to people without having to file for bankruptcy.

328. The length of time between the breach and AMCA's claimed discovery of the Data Breach indicates that AMCA's systems to detect intrusion, detect unusual activity, and log and report such events were inadequate and not in compliance with industry standards. For example, according to technology security company FireEye, the median amount of time between when a data breach occurs and when it is detected was 78 days in 2018. This number has consistently been trending downward in recent years—due to improvements in detection computer technology.[20] The fact that it took AMCA 242 days to detect the Data Breach—nearly 3.5 times the median time for detection in 2018—is direct evidence of its failure to employ reasonable, industry-standard data security practices to safeguard Plaintiffs' and Class Members' Personal Information. AMCA's data security deficiencies would have been readily apparent to Quest had Quest adequately investigated AMCA's data security practices.

329. AMCA's inability to detect its own Data Breach, when an unrelated security firm (Gemini Advisory-which was not working for AMCA) was apparently able to do so with ease, is further evidence of the fact that AMCA employed inadequate data-security practices, and that Quest failed in its independent obligation to ensure that its HIPAA business associate employed reasonable and industry-standard data security measures. The FireEye report indicates that in 2018, the median amount of time that it took a third-party to detect a data breach was three times the median time for internal detection.[21]

---

[20] *M-Trends 2019: FireEye Mandiant Services Special Report*, *available at* https://content.fireeye.com/m-trends (last visited June 11, 2019).

[21] *Id.*

330. One of the easiest ways to minimize exposure to a data breach is to limit the type and amount of information provided to business associates and routine destruction or archiving of inactive PII and PHI so that it cannot not be accessed through online channels. Access to the 11.9 million Quest patient records and 7.7 million LabCorp patient records through AMCA's online portal should not have been possible had AMCA maintained appropriate protections. The sheer number of records suggests that AMCA was not destroying or archiving inactive records. Again, Quest would have discovered this had it exercised adequate oversight over its business associates and audited the data security protocols utilized by AMCA.

331. The Payment Card Industry Security Standards Council promulgates minimum standards, which apply to all organizations that store, process, or transmit payment card data. These standards are known as the Payment Card Industry Data Security Standard ("PCI DSS"). AMCA was not encrypting payment card information according to minimum industry standards of PCI DSS.

332. The payment card industry has published a guide on point-to-point encryption and its benefits in securing payment card data: "point-to-point encryption (P2PE) solution cryptographically protects account data from the point where a merchant accepts the payment card to the secure point of decryption. By using P2PE, account data (cardholder data and sensitive authentication data) is unreadable until it reaches the secure decryption environment, which makes it less valuable if the data is stolen in a breach."[22]

333. Quest had an obligation to exercise oversight over AMCA in a manner that would include immediate knowledge of any data security incidents experienced by AMCA that could

[22] Securing Account Data with the PCI Point –to-Point Encryption Standard v2, available at https://www.pcisecuritystandards.org/documents/P2PE_At_a_Glance_v2.pdf (last accessed June 11, 2019).

affect Quest's patients. For example, AMCA pointed to the fact that it learned of the unauthorized access in March 2019 through a series of CPP notices suggesting that a "disproportionate number of credit cards that at some point had interacted with [AMCA's] web portal were later associated with fraudulent charges." However, Quest did not learn of the unauthorized access until months later in May 2019.

D. Defendants Failed To Provide Proper Notice Of The Data Breach

334. Although Quest was on actual notice of the Data Breach on May 14, 2019 (and should have known about the Data Breach months earlier), it took until June 3, 2019, to publicly acknowledge the breach and months longer to provide notice to impacted customers.

335. On June 3, 2019, Quest publicly acknowledged the Data Breach and indicated that it would be "working with Optum360 to ensure that Quest patients are appropriately notified consistent with the law."[23]

336. However, rather than sending notice directly, Quest relied on AMCA to mail notices to those individuals on its system in June 2019.[24] The notices provided by AMCA were deficient in several respects. First, AMCA's notices failed to indicate to Quest's customers that it was Quest who had given their information to AMCA. Thus, many affected individuals were left to guess why AMCA had their Personal Information in the first instance. Additionally, the notices failed to inform Quest's customers exactly what information had been accessed, thus preventing them from taking measures that could possibly prevent further harm.

[23] Quest Diagnostics Statement on the AMCA Data Security Incident, https://newsroom.questdiagnostics.com/AMCADataSecurityIncident (last visited Oct. 7, 2019).

[24] Quest Diagnostics: July 8, 2019 Notice Unauthorized Access to Database at AMCA Containing Personal Information, https://www.questdiagnostics.com/home/AMCA-data-breach-patients.html (last visited Oct. 7, 2019).

337. It was not until July 8, 2019, almost four months after AMCA received CPP notices, and one month after Quest's first public statement, that Quest put detailed information on its own website regarding the Data Breach and offered credit monitoring to certain affected individuals.[25] But even this effort was deficient in many respects.

a. First, the website indicates that AMCA was the party responsible for sending notice and does not detail any oversight taken by Quest over its business associate.

b. Second, the website limits "complimentary credit monitoring" to those "persons whose Social Security Numbers, credit card information or bank account numbers may have been involved."[26] This limitation means that customers who had other forms of Personal Information taken are not protected. As detailed *infra*, the theft of various forms of Personal Information, not just Social Security Numbers, credit card information, and bank account numbers, can lead to identity theft.

c. Third, Quest acknowledges that there may have been out-of-date contact information for some of its customers. However, Quest provided no means for these customers to obtain information about whether they had been breached and to access credit monitoring. For example, Quest's website does not have any information that its customers can use to determine whether their information was part of the Data Breach.

d. Fourth, Quest's website offered a toll free number that was only available during business hours and for 90 days beginning on July 8, 2019 to allow individuals to "ask questions and learn additional information."[27] This is deficient because (i) the toll-

25 *Id.*

26 *Id.*

27 *Id.*

free number and website are only available for a very short period of time; (ii) the website provides no information about what "questions" or "additional information" can be asked or learned; and (iii) the phone number and website are buried in the website's text, without any emphasis, and under a vague "What We Are Doing" heading and much alter under a "For More Information" heading.

e. Fifth, the website provides no information about the credit monitoring that Quest purported to offer. Rather, it appears to have only been included in some of the mailings and there is no indication to Quest customers on Quest's website of how to sign up for this service or any other relevant details.

338. Further, data breach letters sent by AMCA and Quest to Quest patients further demonstrate the failure to provide proper notice.

a. First, Quest relied on AMCA to provide "24 months of complimentary credit monitoring and identity theft mitigation services." However, providing a clear end point in coverage allows hackers to simply wait out the two years of credit monitoring and then use the relevant information.

b. Second, enrolling into the services is not easy for patients. Rather than being automatically enrolled, patients are required to go through an Equifax website and input a specific activation code. This hurdle is likely to mean that most affected Quest patients do not sign up for the service.

c. Third, neither letter specifically informs patients of what information of theirs was taken. AMCA's letter was limited in its specificity to say: "certain other medical information" was taken. Quest fares little better when it tells patients that the information "may have included" "information related to your providers and the services (such as dates of service,

name of lab, referring doctor, test names, internal patient identification number); and laboratory billing-and payment-related information (such as insurance/payer information and identification number, diagnosis codes, internal account number)."

d. Fourth, Quest's letters did not provide the activation code or even reference that patients could receive the 24 months of complimentary credit monitoring. Patients who only received Quest's letter or went to Quest's website would have no idea that they could receive complimentary credit monitoring.

e. Fifth, Quest should not have relied on AMCA—a bankrupt entity—to be the one to cover credit monitoring costs. It is unclear based on available information whether AMCA can fund the complimentary credit monitoring.

339. In sum, Quest's failure to properly disseminate notice further harmed its customers by keeping them in the dark about whether their information was accessed as a result of the breach, what information was accessed as a result of the breach and how they could quickly and safely respond in order to protect themselves from potential harm as a result of the data breach.

E. Quest Committed To Safeguarding Its Patients' Personal Information

340. Quest's contracts with its patients and policies on its website commit it to protecting patient information, including information shared with third parties.

341. Quest's website makes it clear that it will protect payment information. In response to the question "Is my payment information secure" on its facts and questions page, Quest unequivocally states "yes."[28] Quest promises "Transport Security Layer (TSL) to encrypt your

[28] Quest Diagnostics, https://myquest.questdiagnostics.com/myquest-faq1/QuestDirect.htm (last visited September 27, 2019).

credit card number, name, and address information so only QuestDiagnostics.com is able to decode your information."[29]

342. Quest's privacy policy states that the disclosure of personal information to third parties is limited to "contractors to who we may provide such information for the limited purpose of providing services to us ***and who are obligated to keep the information confidential***."[30]

343. Quest's privacy policy assures that "we limit Quest Diagnostics' employees and contractors' access to personal information. Only those employees and contractors with a business reason to know have access to this information."[31]

344. HIPAA requires that Quest provide every patient it treats, including Plaintiffs and the putative Class Members with a privacy notice. Quest's "Notice of Privacy Practices" acknowledges their legal requirement to maintain the privacy of patients' PHI, and states it is "are committed to protecting the privacy of your identifiable health information."[32] Quest states that "we are required notify affected individuals in the event of a breach involving unsecured protected health information."[33]

---

29 *Id.*

30 Online Privacy Policy, https://www.questdiagnostics.com/home/privacy-policy/online-privacy.html (last visited September 27, 2019) (emphasis added).

31 *Id.*

32 Notice of Privacy Practices, https://www.questdiagnostics.com/home/privacy-policy/notice-privacy-practices.html, (last visited September 27, 2019).

33 *Id.*

345. Quest's Notice of Privacy Policies indicates that it may provide PHI to companies that assist with billing and to "an outside collection agency to obtain payment when necessary."[34] These "business associates" are "***required to maintain the privacy and security of PHI***."[35]

346. The requirements—which stem from contractual duties as well as duties under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")—were violated. Defendants failed to maintain the privacy and security patients PHI and failed to inform patients that their Personal Information was disclosed.

347. Quest also has an Online Privacy Policy where it makes additional promises to its customers regarding the privacy of their Sensitive Information:

> **How We Protect Information Online**
>
> We exercise great care to protect your personal information. This includes, among other things, using industry standard techniques such as firewalls, encryption, and intrusion detection. As a result, while we strive to protect your personal information, we cannot ensure or warrant the security of any information you transmit to us or receive from us. This is especially true for information you transmit to us via email since we have no way of protecting that information until it reaches us since email does not have the security features that are built into our websites.
>
> In addition, we limit Quest Diagnostics' employees and contractors' access to personal information. Only those employees and contractors with a business reason to know have access to this information. We educate our employees about the importance of maintaining confidentiality of customer information.
>
> ***
>
> **Disclosure of Personal Information to Third Parties**
> We will not disclose any personal information to any third party (excluding our contractors to whom we may provide such information for the limited purpose of providing services to us and who are obligated to keep the information confidential), unless (1) you have authorized us to do so; (2) we are legally required to do so, for example, in response to a subpoena, court order or other legal process and/or, (3) it is necessary to protect our property rights related to this website. We also may share aggregate, non-personal information about website usage with

---

34 *Id.*

35 *Id.* (emphasis added).

> unaffiliated third parties. This aggregate information does not contain any personal information about our users.

F. Defendants Violated HIPAA's Requirements To Safeguard Data

348. Defendants had a non-delegable duty to ensure that all information they collected and stored was secure, and that any associated entities with whom they shared member information maintained adequate and commercially reasonable data security practices to ensure the protection of plan members' Personal Information.

349. Defendants are entities covered by HIPAA (*see* 45 C.F.R. § 160.102) and as such are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

350. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. *See* 45 C.F.R. § 160.103.

351. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."

352. HIPAA requires that Defendants implement appropriate safeguards for this information.

353. HIPAA further mandates that a covered entities such as Defendants may disclose PHI to a "business associate," such as AMCA, only if the covered entity obtains satisfactory assurances that the business associate will use the information only for the purposes for which it

was engaged by the covered entity, will safeguard the information from misuse, and assist in compliance with HIPAA privacy obligations.[36]

354. HIPAA requires that Defendants provide notice of a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons – i.e. non-encrypted data.

355. Despite these requirements, Defendants failed to comply with their duties under HIPAA and their own Privacy Practices. Indeed, Defendants failed to:

a. Maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Adequately protect Plaintiffs' and the Class Members' Personal Information;

c. Ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. Implement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

e. Implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

[36] *See* 45 CFR §§ 164.502(e), 164.504(e), 164.532(d) and (e).

f. Implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g. Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

h. Take safeguards to ensure that Defendants' business associates adequately protect protected health information;

i. Ensure compliance with the electronically protected health information security standard rules by their workforces, in violation of 45 C.F.R. § 164.306(a)(4); and/or

j. Train all members of their workforces effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

356. Defendants failed to comply with their duties under HIPAA and their own Codes of Conduct and Privacy Policies despite each being aware of the risks associated with unauthorized access of members' Personal Information.

G. Quest Patients' Personal Information Is Highly Valuable

357. Defendants were or should have been aware that they were collecting highly valuable data, for which Defendants knew or should have known there is an upward trend in data breaches in recent years.[37]

358. The U.S. Department of Health and Human Services, Office for Civil Rights, currently lists 550 breaches affecting 500 or more individuals in the past 24 months.[38] Quest patients are the single largest group impacted by this data breach, exceeding the next lab with impacted patients by over 1.3 million patients. [39]

359. As early as 2014, the FBI alerted the healthcare industry that they were an increasingly preferred target of hackers, stating "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Health Information (PHI) and/or Personally Identifiable Information (PII)" so that these companies can take the necessary precautions to thwart such attacks.[40]

---

[37] Healthcare Data Breach Statistics, HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited September 27, 2019) ("Our healthcare statistics clearly show there has been an upward trend in data breaches over the past 9 years, with 2018 seeing more data breaches reported than any other year since records first started being published.").

[38] U.S. Dep't of Health and Human Services, Office for Civil Rights, *Cases Currently Under Investigation*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited September 27, 2019).

[39] *Id.* Optum360 is listed as the "Covered Entity" and as the Business Associate for Quest, the Healthcare Provider. The next highest is LabCorp (which is also an MDL Defendant and listed as a Healthcare Provider) with just over 10 million patients as a result of the AMCA breach.

[40] Reuters, *FBI warns healthcare firms they are targeted by hackers*, August 20, 2014, http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820 (last visited September 27, 2019).

360. The co-founder of Lastline, a network security provider, said that "[h]ackers target financial companies, like this billing collection company, as they often store sensitive financial information that can be turned into immediate gains."[41]

361. At the end of 2018, the healthcare sector ranked second highest in the number of data breaches among measured sectors, and had the highest rate of exposure for each breach.[42] With this Data Breach, 2019 has seen the exposure of three times the number of records compromised in 2018.[43]

362. Other experts have stated that the Data Breach is at "the intersection of three of the types of data that hackers most desire: personal identifying information that can be used for identity fraud, information about medical conditions, and financial account information."[44]

363. This same article has asked: "why did a collections agency have all of this information in the first place?" It also questioned why medical information and Social Security Numbers needed to be provided to debt collectors.[45]

---

41 Christopher Rowland, Quest Diagnostics discloses breach of patient records, WASH. POST, June 3, 2019, https://www.washingtonpost.com/business/economy/quest-diagnostics-discloses-breach-of-patient-records/2019/06/03/aa37b556-860a-11e9-a870-b9c411dc4312_story.html?utm_term=.78dd30c03a88 (last visited September 27, 2019).

42 Identity Theft Resource Center, 2018 End-of-Year Data Breach Report, https://www.idtheftcenter.org/2018-data-breaches (last visited April 21, 2019).

43 Healthcare Data Breach Statistics (August 2019), HIPPAA Journal, https://www.hipaajournal.com/august-2019-healthcare-data-breach-report (last visited September 27, 2019).

44 Scott Ikeda, Third Party Data Breach Hits Quest Diagnostics with 12 Million Confidential Patient Records Exposed, CPO Magazine, June 11, 2019, https://www.cpomagazine.com/cyber-security/third-party-data-breach-hits-quest-diagnostics-with-12-million-confidential-patient-records-exposed/ (last visited Oct. 7, 2019).

45 *Id.*

364. Further, Cathy Allen, CEO of Shared Assessments, a cyber-risk management group, stated that "just the types of test proscribed might indicate a type of illness that you would not want employers or insurance companies to have. Thieves often steal and resell insurance data on the internet…having other information makes the data more valuable and the price higher."[46] Personal Information is a valuable commodity to identity thieves. Compromised Personal Information is traded on the "cyber black-market." As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, social security numbers and other Personal Information directly on various dark web[47] sites making the information publicly available.[48]

365. Further, medical databases are particularly lucrative targets for identity thieves. According to one report, a stolen medical identity has a $50 street value on the black market, whereas a Social Security number, without more, sells for only $1.[49]

366. Defendants knew or should have known that they had an obligation to take measures to ensure the security of the database maintained by its billing collections vendor because

---

46 *Id.*

47 The dark web refers to encrypted content online that cannot be found using conventional search engines and can only be accessed through specific browsers and software. MacKenzie Sigalos, *The dark web and how to access it* (Apr. 14, 2018), https://www.cnbc.com/2018/04/13/the-dark-web-and-how-to-access-it.html (last accessed June 17, 2019).

48 *Here's How Much Your Personal Information Is Selling for on the Dark Web,* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited November 6, 2019); McFarland et al., *The Hidden Data Economy*, at 3, *available at* https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-data-economy.pdf (last visited November 6, 2019).

49 *Study: Few Aware of Medical Identity Theft Risk*, Claims Journal (June 14, 2012), https://www.claimsjournal.com/news/national/2012/06/14/208510.htm (last visited June 10, 2019).

it contains highly valuable Personal Information and that additional measures to do so were necessary.

H. Defendants Have Harmed Plaintiffs And Class Members By Allowing Anyone To Access Their Information

367. Defendants knew or should have known both that medical information is incredibly valuable to hackers and that health care data breaches are on the rise. Accordingly, Defendants were on notice for the harms that could ensue if they failed to protect patients' data.

368. Quest, moreover, had previously failed to protect patients' private information. In 2016, Quest allowed an unauthorized third party to access its internal internet application and obtain the protected health information of 34,000 individuals.[50] This data included name, date of birth, lab results, and in some instances, phone numbers.[51] At that time, a company spokesman said that "we're taking it seriously."[52]

369. In October 2019, the United States District Court for the District of New Jersey preliminarily approved a settlement related to this 2016 breach allowing for up to a $325 reimbursement for each class member.

370. Given the sensitive nature of the Personal Information stolen in the Data Breach – including names, mailing addresses, phone numbers, dates of birth, Social Security numbers, information related to Plaintiffs' and Class Members' medical providers and services (such as dates of service, name of lab, referring doctor, test names, internal patient identification number),

---

50 http://ir.questdiagnostics.com/news-releases/news-release-details/quest-diagnostics-provides-notice-data-security-incident?ID=2229113&c=82068&p=irol-newsArticle.

51 *Id.*

52 Robert Channick, Quest data breach exposes private health information of 34,000 patients, Chicago Tribune, Dec. 13, 2016, https://www.chicagotribune.com/business/ct-quest-data-hack-1214-biz-20161213-story.html.

diagnosis codes, credit and debit card numbers, bank account information, and insurance policy numbers – hackers have the ability to commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and Class Members now and into the indefinite future.

371. In fact, many victims of the Data Breach have already experienced harms as the result of the Data Breach, including, but not limited to, identity theft, financial fraud, tax fraud, unauthorized lines of credit opened in their names, medical and healthcare fraud, and unauthorized access to their bank accounts. Plaintiffs and Class Members have also spent time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit protection services, contacting their financial institutions, checking credit reports, and spending time and effort searching for unauthorized activity.

372. The Personal Information exposed in the Data Breach is highly coveted and valuable on underground or black markets. For example, a cyber "black market" exists in which criminals openly post and sell stolen consumer information on underground internet websites known as the "dark web" – and information tied to this Data Breach has already been offered for sale. Identity thieves can use the Personal Information to: (a) create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards; (b) reproduce stolen debit cards and use them to withdraw cash from ATMs; (c) commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits; (f) file a fraudulent tax return using the victim's information; (g) commit medical and healthcare-related fraud; (h) access financial accounts and records; or (i) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest. Further, loss of private and personal health information can expose the victim to loss of reputation, loss of employment, blackmail, extortion, and other negative effects.

373. In a data breach implicating a medical provider or medical information, consumers face the additional risk of their Health Savings Accounts ("HSAs") being compromised. HSAs are often tied to specialized debit cards used to make medical-based payments. However, they can also be used for regular purchases (albeit incurring a severe tax penalty). Such information is an "easy target" for criminal actors.[53]

374. As AMCA acknowledged, fraudulent charges have already been linked to the data Quest provided to AMCA. Quest publicly revealed the exposure of patients' Personal Information only after "a disproportionate number of credit cards that at some point had interacted with [AMCA's] web portal were later associated with fraudulent charges."[54]

375. In addition, the impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 described that the identity theft they experienced affected their ability to get credit cards and obtain loans, such as student loans or mortgages.[55] For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

376. As explained further by the FTC, medical identity theft can have other serious consequences:

> Medical ID thieves may use your identity to get treatment – even surgery – or to bilk insurers by making fake claims. Repairing damage to your good name and

---

53 *Id.*

54 Declaration of Russell H. Fuchs Pursuant to Local Bankruptcy Rule 1007-2 And In Support Of "First Day" Motions, American Medical Collection Agency Bankruptcy Petition #19-23185(RDD), Docket Entry 2 (Bankr. S.D.N.Y.)

55 Identity Theft Resource Center, *The Aftermath 2017*, https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited Aug. 9, 2019).

> credit record can be difficult enough, but medical ID theft can have other serious consequences. If a scammer gets treatment in your name, that person's health problems could become a part of your medical record. It could affect your ability to get medical care and insurance benefits, and could even affect decisions made by doctors treating you later on. The scammer's unpaid medical debts also could end up on your credit report.[56]

377. As the result of the wide variety of injuries that can be traced to the Data Breach, Plaintiffs and Class Members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. losing the inherent value of their Personal Information;

b. identity theft and fraud resulting from the theft of their Personal Information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

e. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

f. lowered credit scores resulting from credit inquiries following fraudulent activities;

g. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts; and

h. the continued imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being in the possession of one or many unauthorized third parties.

---

[56] *Medical ID Theft: Health Information for Older People*, Federal Trade Commission, *available at* https://www.consumer.ftc.gov/articles/0326-medical-id-theft-health-information-older-people (last visited October 7, 2019).

378. Even in instances where a consumer is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement that is not refunded. The Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" relating to identity theft or fraud.[57]

379. There may also be a significant time lag between when personal information is stolen and when it is actually misused. According to the GAO, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[58]

380. Plaintiffs and Class Members place significant value in data security. According to a recent survey conducted by cyber-security company FireEye, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[59]

---

[57] E. Harrell, U.S. Department of Justice, *Victims of Identity Theft, 2014* (revised Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited Aug. 9, 2019).

[58] U.S. Gov't Accountability Off., GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent Is Unknown* (2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited Aug. 9, 2019).

[59] FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 2016), https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last visited Aug. 9, 2019).

381. Because of the value consumers place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if consumers did not value their data security and privacy, Defendants would have no reason to tout their data security efforts to their actual and potential customers.

382. Consequently, had consumers known the truth about Defendants' data security practices – that they did not adequately protect and store their Personal Information – they would not have entrusted their Personal Information to Quest.

383. Quest's failure to protect Plaintiffs' and Class Members' personal data has led to significant governmental investigation. Specifically, on June 5, 2019, New Jersey's United States Senators Corey Booker and Bob Menendez sent a letter to Quest's Chairman, President & CEO stating that they were "deeply concerned" and asking for detailed information about the breach, Quest's responses, and Quest's data security processes.[60]

384. Separately, the Attorneys General of Connecticut and Illinois opened an investigation on June 7, 2019 into Quest and LabCorp. In a press release, they stated: The last thing patients should have to worry about is whether their personal information has been compromised by the entities responsible for protecting it. I am committed to ensuring that impacted patients receive timely notification and that the companies involved take precautions to protect consumers' sensitive health and financial information in the future.[61] Michigan's Attorney

---

[60] Letter from U.S. Senators Robert Menendez and Cory A. Booker (June 5, 2019), *available at* https://www.menendez.senate.gov/imo/media/doc/06.05.19%20LabCorp%20Letter.pdf

[61] Connecticut and Illinois Open Investigation into Quest Diagnostics, LabCorp Data Breach, The Office of Attorney General William Tong, available at https://portal.ct.gov/AG/Press-Releases/2019-Press-Releases/CT-AND-IL-OPEN-INVESTIGATION-INTO-QUEST-AND-LABCORP-DATA-BREACH.

General also launched an investigation shortly after the Data Breach was announced.[62] In its recent quarterly SEC filing, Quest acknowledged that "certain federal and state governmental authorities are investigating, or otherwise seeking information and/or documents from the Company related to the AMCA Data Security Incident and related matters, including Attorneys General offices from numerous states and the District of Columbia and certain U.S. senators."[63]

CLASS ACTION ALLEGATIONS

I. NATIONWIDE CLASS

385. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of the following nationwide class (the "Nationwide Class" or the "Class"):

> All natural persons residing in the United States whose Personal Information was compromised in the Data Breach.

386. The Nationwide Class asserts claims against Defendants for negligence (Count 1), negligence *per se* (Count 2), unjust enrichment (Count 3), declaratory judgment (Count 4), breach of implied contract (Count 5), violations of the New Jersey Consumer Fraud Act, N.J.S.A. § 56:8-1, *et seq*. (Count 6), violations of the Minnesota Consumer Fraud Act, Minn. Stat. §§ 325F.68, *et seq*. and Minn. Stat. §§ 8.31, *et seq.* (Count 7), and violations of the Minnesota Uniform Deceptive Trade Practices Act, Minn. Stat. §§ 325D.43, *et seq.* (Count 8).

---

[62] AMCA Data Breach Tally Passes 20 Million as BioReference Laboratories Added to List of Impacted Entities, HIPPA Journal, https://www.hipaajournal.com/amca-data-breach-tally-passes-20-million-as-bioreference-laboratories-added-to-list-of-impacted-entities/ (last visited October 9, 2019).

[63] Quest Diagnostics, Inc. Form 10-Q (Oct. 23, 2019), http://d18rn0p25nwr6d.cloudfront.net/CIK-0001022079/9fd46d10-0cf2-4eb7-9140-c903f6b5c641.pdf

II. STATEWIDE SUBCLASSES

387. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of state-by-state claims in the alternative to the nationwide claims, as well as statutory claims under state data breach statutes and consumer protection statutes (Counts 8 through 32), on behalf of separate statewide subclasses for each State (the "Statewide Subclasses"), defined as follows:

> All natural persons residing in [name of state] whose Personal Information was compromised in the Data Breach.

388. Excluded from the Nationwide Class and each Statewide Subclass are Defendants, any entity in which either Defendant has a controlling interest, and either Defendants' officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Nationwide Class and each Statewide Subclass are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

389. **Numerosity: Federal Rule of Civil Procedure 23(a)(1)**. The members of each Class and Subclass are so numerous and geographically dispersed that individual joinder of all Class Members is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, Defendants have acknowledged that millions of Quest customers' Personal Information has been compromised. Those individuals' names and addresses are available from Defendants' records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods. On information and belief, there are at least thousands of Class Members in each Statewide Subclass, making joinder of all Statewide Subclass members impracticable.

390. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and

fact that predominate over any questions affecting individual Class Members. The common questions include:

a. Whether Defendants had a duty to protect Personal Information;

b. Whether Defendants failed to take reasonable and prudent security measures;

c. Whether Defendants knew or should have known of the susceptibility of AMCA's systems to a data breach;

d. Whether Defendants were negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Defendants' security measures to protect its systems were reasonable in light known legal requirements;

f. Whether Defendants were negligent in failing to adequately monitor and audit the data security systems of their vendors and business associates;

g. Whether Defendants' efforts (or lack thereof) to ensure the security of patients' Personal Information provided to vendors and business associates were reasonable in light of known legal requirements;

h. Whether Defendants' conduct constituted unfair or deceptive trade practices;

i. Whether Defendants violated state law when they failed to implement reasonable security procedures and practices;

j. Which security procedures and notification procedures Defendants should be required to implement;

k. Whether Defendants have a contractual obligation to use reasonable security measures;

l. Whether Defendants have complied with any contractual obligation to use reasonable security measures;

m. What security measures, if any, must be implemented by Defendants to comply with their contractual obligations;

n. Whether Defendants violated state consumer protection and state medical information privacy laws in connection with the actions described herein;

o. Whether Defendants failed to notify Plaintiffs and Class Members as soon as practicable and without delay after the data breach was discovered;

p. Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the breach of AMCA's systems and/or the loss of the Personal Information of Plaintiffs and Class Members;

q. Whether Plaintiffs and Class Members were injured and suffered damages or other losses because of Defendants' failure to reasonably protect their Personal Information; and,

r. Whether Plaintiffs and Class Members are entitled to damages, declaratory or injunctive relief.

391. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiffs' claims are typical of those of other Class Members. Plaintiffs' Personal Information was in Defendants' possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiffs' damages and injuries are akin to other Class Members and Plaintiffs seek relief consistent with the relief of the Class.

392. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiffs are adequate representatives of the Class because Plaintiffs are members of the Class and are committed to pursuing this matter against Defendants to obtain relief for the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

393. **Predominance & Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. Common issues in this litigation also predominate over individual issues because those issues discussed in the above paragraph on commonality are more important to the resolution of this litigation than any individual issues. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Defendants, and thus, individual litigation to redress Defendants' wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

394. **Risk of Prosecuting Separate Actions.** This case is appropriate for certification because prosecuting separate actions by individual proposed Class Members would create the risk of inconsistent adjudications and incompatible standards of conduct for Defendants or would be dispositive of the interests of members of the proposed Class.

395. **Ascertainability.** The Class and Subclasses are defined by reference to objective criteria, and there is an administratively feasible mechanism to determine who fits within the class. The Class and Subclasses consist of individuals who received services from Quest and whose accounts were placed into collections with AMCA by Quest. Class Membership can be determined using Quest and AMCA's records in their databases.

396. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendants, through their uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole. Injunctive relief is necessary to uniformly protect the Class Members' data. Plaintiff seeks prospective injunctive relief as a wholly separate remedy from any monetary relief.

397. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Personal Information;

b. Whether Defendants failed to take commercially reasonable steps to safeguard the Personal Information of Plaintiffs and the Class Members;

c. Whether Defendants failed to adequately monitor and audit the data security systems of their vendors and business associates;

d. Whether adherence to HIPAA regulations, FTC data security recommendations, industry standards, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CHOICE OF LAW FOR NATIONWIDE CLAIMS

398. The state laws of one state will likely govern Plaintiffs' claims.

399. **New Jersey:** First, Secaucus, New Jersey, Quest's principal place of business, is the "nerve center" of its business activities—the place where its high-level officers direct, control, and coordinate the corporation's activities, including its data security functions and major policy, financial, and legal decisions.

400. New Jersey has significant interests in regulating the conduct of businesses operating within its borders. New Jersey, which seeks to protect the rights and interests of residents and citizens of the United States against a company headquartered and doing business there, has a greater interest in the nationwide claims of Plaintiffs and Class Members as to the conduct of Quest than any other state and is most intimately concerned with the claims and outcome of this litigation.

401. Quest's response to the Data Breach at issue here, and corporate decisions surrounding such response, were made from and in New Jersey.

402. Quest's breaches of duty to Plaintiffs and Nationwide Class Members emanated from New Jersey.

403. **Minnesota:** Second, Eden Prairie, Minnesota, Optum 360's principal place of business, is the "nerve center" of its business activities—the place where its high-level officers

direct, control, and coordinate the corporation's activities, including its data security functions and major policy, financial, and legal decisions.

404. Minnesota has significant interests in regulating the conduct of businesses operating within its borders. Minnesota, which seeks to protect the rights and interests of residents and citizens of the United States against a company headquartered and doing business there, has a greater interest in the nationwide claims of Plaintiffs and Class Members as to the conduct of Optum360 LLP than any other state and is most intimately concerned with the claims and outcome of this litigation.

405. Optum360 LLP's response to the Data Breach at issue here, and corporate decisions surrounding such response, were made from and in Minnesota.

406. Optum360 LLP's breaches of duty to Plaintiffs and Nationwide Class members emanated from Minnesota.

407. Additional factual analysis is necessary in order to determine which state's law should apply to the claims of the Class Members. Accordingly, it would be inappropriate to determine choice of law at the pleadings stage of this case. Plaintiffs are therefore pleading nationwide claims based upon New Jersey and Minnesota law in the alternative (or under the law of the states of each Plaintiff).

408. Application of New Jersey or Minnesota law with respect to Plaintiffs' and Class Members' claims after the completion of a factual inquiry would be neither arbitrary nor fundamentally unfair because New Jersey and Minnesota each has significant contacts and a significant aggregation of contacts that create a state interest in the claims of Plaintiffs and class members as to the conduct of the respective Defendants.

409. Under choice of law principles applicable to this action, the common law of New Jersey or Minnesota would apply to the nationwide common law claims of all Class Members given New Jersey's and Minnesota's significant interests in regulating the conduct of businesses operating within their borders, consumer protection laws may be applied to non-resident consumer plaintiffs upon completion of the factual analysis required for the choice of law determination.

410. To the extent the Court finds that the laws of each Class Member's state apply to his or her injuries, Plaintiffs previously provided Defendants with notice sufficient to satisfy state statutory requirements, and sent correspondence to Defendants' counsel on November 14, 2019 providing the company with additional information on Plaintiffs' claim.

CLAIMS ON BEHALF OF THE NATIONWIDE CLASS

COUNT 1

NEGLIGENCE

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

411. Plaintiffs repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

412. Quest required Plaintiffs and Class Members to submit Personal Information to obtain diagnostic and medical services, which Quest provided to Optum360 and its vendor AMCA for billing purposes. Defendants collected and stored the Personal Information for commercial gain.

413. Defendants knew or should have known that AMCA's web payments page was vulnerable to unauthorized access by third parties.

414. Defendants had a non-delegable duty to ensure that contractual partners with whom they shared patient information maintained adequate and commercially reasonable data security practices to ensure the protection of patients' Personal Information.

415. Defendants owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and Class Members' Personal Information within their control from being compromised, lost, stolen, accessed and misused by unauthorized persons.

416. Defendants owed a duty of care to Plaintiffs and Class Members to provide security, consistent with industry standards, to ensure that the systems and networks adequately protected the Personal Information.

417. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants and the Plaintiffs and Class Members. The special relationship arose because Plaintiffs and Class Members entrusted Defendants with their confidential data as part of the health treatment process. Only Defendants were in a position to ensure that their contractual partners had sufficient safeguards to protect against the harm to Plaintiffs and Class Members that would result from a data breach.

418. Defendants' duty to use reasonable care in protecting Personal Information arose as a result of the common law and the statutes and regulations, as well as their own promises regarding privacy and data security to Quest's patients. This duty exists because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices. By collecting and maintaining personal and confidential information of Plaintiffs and Class Members, and acknowledging that this information needed to be kept secure, it was foreseeable that they would be harmed in the future if Defendants did not protect Plaintiffs' and Class Members' information from hackers.

419. Defendants' duties also arose under HIPPA regulations, which, as described above, applied to Defendants and establish national standards for the protection of patient information,

including protected health information, which required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The duty also arose under HIPAA's Privacy Rule requirement that Defendants obtain satisfactory assurances from their business associate AMCA that AMCA would appropriately safeguard the protected health information it receives or creates on behalf of the Defendants. 45 CFR 164.502(e), 164.504(e), 164.532(d) and (e). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

420. Defendants' duties also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal and confidential information. Various FTC publications and data security breach orders further form the basis of Defendants' duty. In addition, several individual states have enacted statutes based upon the FTC Act that also created a duty.

421. Defendants knew, or should have known, of the risks inherent in collecting and storing Personal Information, the vulnerabilities of its vendors and business associates' systems, and the importance of adequate security. Quest specifically knew about the risks inherent in collecting and storing Personal Information given its experience with a recent cyber-attack in November 2016 and its acknowledgment that Quest's "business associates" are "required to maintain the privacy and security of [patients'] PHI."

422. Defendants breached their common law, statutory, and other duties – and thus were negligent-–by failing to use reasonable measures to protect patients' Personal Information, and by failing to provide timely and adequately detailed notice of the Data Breach.

423. Defendants breached their duties to Plaintiffs and Class Members in numerous ways, including by:

a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect Plaintiffs' and Class Members' Personal Information;

b. Failing to comply with industry standard data security standards during the period of the Data Breach;

c. Failing to comply with regulations protecting the Personal Information at issue during the period of the Data Breach;

d. Failing to adequately monitor and audit the data security systems of its vendors and business associates;

e. Failing to adequately monitor, evaluate, and ensure the security of AMCA's network and systems;

f. Failing to recognize in a timely manner that Plaintiffs' and other Class Members' Personal Information had been compromised; and

g. Failing to timely and adequately disclose that Plaintiffs' and Class Members' Personal Information had been improperly acquired or accessed.

424. Plaintiffs' and Class Members' Personal Information would not have been compromised but for Defendants' wrongful and negligent breach of their duties.

425. Defendants' failure to take proper security measures to protect sensitive Personal Information of Plaintiffs and Class Members created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiffs' and Class Members' Personal Information.

426. It was also foreseeable that Defendants' failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiffs and Class Members as described in this Complaint.

427. Neither Plaintiffs nor the other Class Members contributed to the Data Breach and subsequent misuse of their Personal Information.

428. As a direct and proximate cause of Defendants' conduct, Plaintiffs and Class Members suffered damages and will suffer damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the Personal Information of Plaintiff and Class Members; damages arising from identity theft or fraud; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take years to discover and detect; and loss of the value of their privacy and confidentiality of the stolen confidential data, including health data.

COUNT 2

NEGLIGENCE PER SE
On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

429. Plaintiffs repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

430. Defendants are entities covered by HIPAA (45 C.F.R. § 160.102) and as such are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"),

and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

431. HIPAA requires Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). HIPAA also requires Defendants to obtain satisfactory assurances that its business associates would appropriately safeguard the protected health information it receives or creates on behalf of the Defendants. 45 CFR § 164.502(e), 164.504(e), 164.532(d) and (e). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA. AMCA constitutes a "business associate" within the meaning of HIPAA.

432. HIPAA further requires Defendants to disclose the unauthorized access and theft of the Personal Information to Plaintiff and Class Members "without unreasonable delay" so that Plaintiffs and Class Members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Personal Information. *See* 45 C.F.R. §§ 164.404, 406, 410.

433. Defendants violated HIPAA by failing to reasonably protect Plaintiffs' and Class Members' Personal Information, as described herein.

434. Defendants' violations of HIPAA constitute negligence per se.

435. Plaintiffs and Class Members are within the class of persons that HIPAA was intended to protect.

436. The harm that occurred as a result of the Data Breach is the type of harm HIPAA was intended to guard against.

437. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect Personal Information. 15 U.S.C. § 45(a)(1).

438. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

439. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of Personal Information it obtained, stored, and disseminated, and the foreseeable consequences of a data breach involving companies as large as Quest, including, specifically, the immense damages that would result to Plaintiffs and Class Members.

440. Defendants' violations of Section 5 of the FTC Act constitute negligence per se.

441. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

442. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members.

443. As a direct and proximate result of Defendants' negligence per se under HIPAA and the FTC Act, Plaintiffs and the Class have suffered, continue to suffer, and will suffer, injuries, damages, and harm as set forth herein.

COUNT 3

UNJUST ENRICHMENT
On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

444. Plaintiffs repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

445. Plaintiffs and Class Members have an interest, both equitable and legal, in the Personal Information about them that was conferred upon, collected by, and maintained by Defendants and which was ultimately stolen in the Data Breach.

446. Defendants received a monetary benefit from Plaintiff and Class Members conferring upon them their Personal Information, which Defendants retain and use for business purposes and profit.

447. Plaintiffs' and Class Members' Personal Information was private and confidential and its value depended upon Defendants maintaining the privacy and confidentiality of that Personal Information.

448. But for Quest's commitment to maintain the confidentiality and security of their Personal Information, Plaintiffs and Class Members would not have provided the information to Quest.

449. As a result of the wrongful conduct alleged herein, Defendants have been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class Members. Among other things, Defendants continue to benefit and profit from the use of Plaintiffs' and Class Members' Personal Information, while its value to Plaintiffs and Class Members has been diminished and its exposure has caused Plaintiffs and Class Members harm.

450. Under the doctrine of unjust enrichment, it is inequitable for Defendants to be permitted to retain the benefits they received, and are still receiving, from Plaintiffs and Class Members.

451. Equity and good conscience require restitution by the Defendants in the amount of the benefit conferred on Defendants as a result of their wrongful conduct, including, specifically, the value to Defendants of the Personal Information that was stolen in the Data Breach and the resulting profits Defendants received and are receiving from the use of that information.

COUNT 4

DECLARATORY JUDGMENT

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

452. Plaintiffs repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

453. As previously alleged, Plaintiffs and Class Members entered into an implied contract that required Defendants to provide adequate security for the Personal Information it collected from them. As previously alleged, Defendants owe duties of care to Plaintiff and Class Members that require them to adequately secure Personal Information.

454. Defendants still possess Personal Information pertaining to Plaintiffs and Class Members.

455. Defendants have made no announcement or notification that they have remedied the vulnerabilities in their practices and policies regarding ensuring the data security of patients' Personal Information.

456. Accordingly, Defendants have not satisfied their implied contractual allegations and legal duties to Plaintiffs and Class Members. In fact, now that Defendants' lax approach towards data security has become public, the Personal Information in their possession and in their

vendors and business associates' possession is more vulnerable than it was prior to announcement of the Data Breach.

457. Actual harm has arisen in the wake of the Data Breach regarding Defendants' contractual obligations and duties of care to provide data security measures to Plaintiffs and Class Members, including the fact that Class Members' Personal Information was available for sale on the dark web.

458. Plaintiffs, therefore, seek a declaration that (a) Defendants' existing data security measures do not comply with their obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

a. Modifying their practices and policies to ensure the vendors and business associates to which they provide patients' Personal Information engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on their systems on a periodic basis, and ordering vendors and business associates to promptly correct any problems or issues detected by such third-party security auditors;

b. Modifying their practices and policies to ensure the vendors and business associates to which they provide patients' Personal Information engage third-party security auditors and internal personnel to run automated security monitoring;

c. Modifying their practices and policies to ensure the vendors and business associates to which they provide patients' Personal Information audit, test, and train security personnel regarding any new or modified procedures;

d. Modifying their practices and policies to ensure the vendors and business associates to which they provide patients' Personal Information segment Personal Information by, among other things, creating firewalls and access controls so that if one area of a system is compromised, hackers cannot gain access to other portions of the systems;

e. Modifying their practices and policies to ensure only Personal Information necessary for provision of services is provided to vendors and business associates;

f. Modifying their practices and policies to ensure Personal Information not necessary for the provision of services is purged, deleted, and destroyed, and to ensure its vendors and business associates likewise purge, delete, and destroy such Personal Information;

g. Conducting regular security checks of the vendors and business associates to which it provides patients' Personal Information;

h. Routinely and continually conduct internal training and education to inform internal security personnel how to monitor the data security of vendors and business associates to whom patients' Personal Information is provided; and

i. Educating its patients about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Defendants' patients must take to protect themselves.

COUNT 5

BREACH OF IMPLIED CONTRACT

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

459. Plaintiffs repeat the allegations set forth in the preceding paragraphs as if fully set forth herein.

460. Plaintiffs and Class Members were required to provide their Personal Information, including names, addresses, Social Security numbers, financial information, and other personal information, to Quest in order to complete medical and diagnostic tests.

461. When Plaintiffs and Class Members provided their Personal Information to Quest in exchange for services, they entered into implied contracts with Quest and its business associate, Optum360, pursuant to which Defendants agreed to safeguard and protect such information and to timely and adequately notify them if their data had been breached and compromised.

462. Plaintiffs and the Class Members would not have provided and entrusted their Personal Information to Defendants in the absence of the implied contract to keep the information secure.

463. Plaintiffs and the Class Members fully performed their obligations under the implied contract with Defendants by providing their Personal Information, whereas Defendants did not comply with their obligations to keep the information secure.

464. Defendants breached the implied contracts with Plaintiffs and Class Members by failing to reasonably safeguard and protect Plaintiffs and Class Members' Personal Information, which was compromised as a result of the Data Breach.

465. As a direct and proximate result of Defendants' breach of their implied contacts with Plaintiffs and Class Members, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity as to how their Personal Information is used; (ii) the compromise, publication, and/or theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate

the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) the continued risk to their Personal Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Personal Information in their continued possession; and, (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

COUNT 6

NEW JERSEY CONSUMER FRAUD ACT, N.J.S.A. § 56:8-1, *et seq.*
On Behalf of Plaintiffs and the Nationwide Class against Defendant Quest, or Alternatively, on Behalf of the New Jersey Subclass against Both Defendants

466. Plaintiffs repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

467. The New Jersey Consumer Fraud Act (the "NJCFA"), N.J.S.A. § 56:8-1, *et seq*., prohibits the act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression or omission, in connection with the sale or advertisement of any merchandise. The NJCFA applies whether or not any person has in fact been misled, deceived or damaged thereby. N.J.S.A. § 56:8-2.

468. Plaintiffs, Defendants, and Class Members are "persons" within the meaning of N.J.S.A. § 56:8-1(d).

469. Defendants sell "merchandise," as defined by N.J.S.A. § 56:8-1, by offering health benefits services to the public.

470. Defendants, operating in New Jersey, engaged in unconscionable and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of health benefits services in violation of N.J.S.A. § 56:8-2, including but not limited to the following:

a. Misrepresenting material facts, pertaining to the sale of health benefits services, to the Plaintiffs and Class Members by representing that they would maintain adequate data security practices and procedures to safeguard Plaintiffs' and Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;

b. Misrepresenting material facts, pertaining to the sale of health benefits services, to the Plaintiffs and Class Members by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiffs' and Class Members' Personal Information;

c. Knowingly omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiffs' and Class Members' Personal Information with the intent that Plaintiffs and Class Members rely on the omission, suppression, and concealment;

d. Engaging in unconscionable and deceptive acts and practices with respect to the sale of health benefit services by failing to adequately monitor and audit the data security systems of its vendors and business associates and failing to maintain the privacy and security of Plaintiffs and Class Members' Personal Information in violation of duties imposed by and public policies reflected in the FTC Act and HIPAA;

e. Engaging in unconscionable and deceptive acts and practices by failing to disclose the Data Breach to Plaintiffs and Class Members in a timely and accurate manner in violation of N.J.S.A. § 56:8-163;

f. Advertising Quest's medical treatments with the intent not to sell it as advertise—*i.e*. with worse data security than advertised; and

g. Representing on its website that it is "committed to protecting the privacy of your identifiable health information," when, in fact, Quest failed to safeguard customers' information by providing it to AMCA, which had deficient data security protection.

471. The above unlawful and deceptive acts and practices by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

472. Defendants knew or should have known that their data security practices were inadequate to safeguard Plaintiffs' and Class Members' Personal Information and that the risk of a data breach was highly likely. Defendants' actions in engaging in the above-listed unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and Class Members.

473. Plaintiffs and Class Members reasonably expected that Defendants would protect their Personal Information and reasonably expected that Defendants would provide truthful statements on their website and privacy policies, and that it would be safe to provide Quest with their information. These representations and affirmations of fact made by Defendants, and the facts they concealed or failed to disclose, are material facts that were likely to deceive reasonable consumers, and that reasonable consumers would, and did, rely upon in deciding whether or not

to provide their information to Quest. Defendants, moreover, intended for consumers, including Plaintiffs and Class Members, to rely on these material facts.

474. As a direct and proximate result of Defendants' unconscionable and deceptive acts and practices, Plaintiffs and Class Members suffered an ascertainable loss in moneys or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.

475. Plaintiffs and Class Members seek relief under N.J.S.A. § 56:8-19, including but not limited to, injunctive relief, other equitable relief, actual damages, treble damages, and attorneys' fees and costs.

COUNT 7

MINNESOTA CONSUMER FRAUD ACT,
Minn. Stat. §§ 325F.68, *et seq*. and Minn. Stat. §§ 8.31, *et seq.*
On Behalf of Plaintiffs and the Nationwide Class against Defendant Optum360, or Alternatively, on Behalf of the Minnesota Subclass against Both Defendants

476. Plaintiffs repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

477. Defendants, Plaintiffs, and Class Members are each a "person" as defined by Minn. Stat. § 325F.68(3).

478. Defendants' goods, services, commodities, and intangibles are "merchandise" as defined by Minn. Stat. § 325F.68(2).

479. Defendants engaged in "sales" as defined by Minn. Stat. § 325F.68(4).

480. Defendants engaged in fraud, false pretense, false promise, misrepresentation, misleading statements, and deceptive practices in connection with the sale of merchandise, in violation of Minn. Stat. § 325F.69(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' Personal Information, including by implementing and maintaining reasonable security measures and ensuring its vendors and business associates maintained reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' Personal Information or ensure its vendors and business associates reasonably or adequately secured such information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Class Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA.

481. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

482. Defendants intended to mislead Plaintiffs and Class Members and induce them to rely on their misrepresentations and omissions.

483. Defendants' fraudulent, misleading, and deceptive practices affected the public interest, including those affected by the Data Breach.

484. As a direct and proximate result of Defendants' fraudulent, misleading, and deceptive practices, Plaintiffs and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

485. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including damages; injunctive or other equitable relief; and attorneys' fees, disbursements, and costs.

COUNT 8

MINNESOTA UNIFORM DECEPTIVE TRADE PRACTICES ACT, Minn. Stat. §§ 325D.43, *et seq.*

On Behalf of Plaintiffs and the Nationwide Class against Defendant Optum360, or Alternatively, on Behalf of the Minnesota Subclass against Both Defendants

486. Plaintiffs repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

487. By engaging in deceptive trade practices in the course of their businesses and vocations, directly or indirectly affecting the people of Minnesota, Defendants violated Minn. Stat. § 325D.44, including the following provisions:

a. Representing that their goods and services had characteristics, uses, and benefits that they did not have, in violation of Minn. Stat. § 325D.44(1)(5);

b. Representing that goods and services are of a particular standard or quality when they are of another, in violation of Minn. Stat. § 325D.44(1)(7);

c. Advertising goods and services with intent not to sell them as advertised, in violation of Minn. Stat. § 325D.44(1)(9); and

d. Engaging in other conduct which similarly creates a likelihood of confusion or misunderstanding, in violation of Minn. Stat. § 325D.44(1)(13).

488. Defendants' deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Class Members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy

measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs and Class Members' Personal Information, including by implementing and maintaining reasonable security measures and ensuring their vendors and business associates maintained reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs and Class Members' Personal Information or ensure their vendors and business associates reasonably or adequately secured such information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA.

489. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

490. Defendants intended to mislead Plaintiff and Class Members and induce them to rely on their misrepresentations and omissions.

491. Had Defendants disclosed to Plaintiffs and Class members that AMCA's data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and they would have been forced to use vendors and business associates with reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and Class Members' Personal Information as part of the services they provided without advising Plaintiffs and Class Members that AMCA's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Class Members' Personal Information. Accordingly, Plaintiffs and Class Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

492. Defendants acted intentionally, knowingly, and maliciously to violate Minnesota's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiffs' and Class Members' rights. Quest's past data breaches and breaches within the medical industry put them on notice that their security and privacy protections were inadequate.

493. As a direct and proximate result of Defendants' deceptive trade practices, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to

monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

494. Plaintiffs and Class Members seek all relief allowed by law, including injunctive relief and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS

COUNT 9

CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, Cal. Civ. Code §§ 56, *et seq.*

495. The California Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

496. California's Confidentiality of Medical Information Act ("CMIA") requires a healthcare provider "who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information [to] do so in a manner that preserves the confidentiality of the information contained therein." Cal. Civ. Code § 56.101. "Every provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36." *Id.*

497. The CMIA further requires that "[a]n electronic health record system or electronic medical record system . . . [p]rotect and preserve the integrity of electronic medical information." Cal. Civ. Code § 56.101(b)(1)(A).

498. Plaintiff and California Subclass members are "patient[s]," "whether or not still living, who received health care services from a provider of health care and to whom medical information pertains" pursuant to § 56.05(k) of the CMIA.

499. Defendants are each a "provider of healthcare" pursuant to § 56.05(m) of the CMIA "who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information."

500. Defendants are subject to the requirements and mandates of the CMIA.

501. The Personal Information of Plaintiff and California Subclass members compromised in the Data Breach constitutes "medical information" maintained in electronic form pursuant to § 56.05(j) of the CMIA.

502. Defendants violated § 56.36(b) of the CMIA by negligently maintaining, preserving, storing and releasing the Personal Information of Plaintiff and California Subclass members, and failing to protect and preserve the integrity of the Personal Information of Plaintiff and California Subclass members.

503. Plaintiff and California Subclass members did not authorize Defendants' disclosure and release of their Personal Information that occurred in the Data Breach.

504. As a result of the Data Breach, the Personal Information of Plaintiff and California Subclass members was compromised when it was acquired and accessed by unauthorized parties.

505. Defendants violated the CMIA by negligently (1) failing to implement reasonable administrative, physical and technical safeguards to protect, secure and prevent the unauthorized access to, and acquisition of, Plaintiff's and California Subclass members' Personal Information; (2) failing to implement reasonable data security measures, such as intrusion detection processes that detect data breaches in a timely manner, to protect and secure Plaintiff's and California Subclass members' Personal Information and ensuring their vendors and business associates implemented such measures; (3) failing to use reasonable authentication procedures to track Personal Information in case of a security breach and ensuring their vendors and business

associates implemented such measures; and (4) allowing undetected and unauthorized access to servers, networks and systems where Plaintiff's and California Subclass members' Personal Information was kept.

506. Defendants' failure to implement adequate data security measures to protect the Personal Information of Plaintiff and California Subclass members was a substantial factor in allowing unauthorized parties to access AMCA's computer systems and acquire the Personal Information of Plaintiff and California Subclass members.

507. As a direct and proximate result of Defendants' violation of the CMIA, Defendants allowed the Personal Information of Plaintiff and California Subclass members to: (a) escape and spread from its normal place of storage through unauthorized disclosure or release; and (b) be accessed and acquired by unauthorized parties in order to, on information and belief, view, mine, exploit, use, and/or profit from their Personal Information, thereby breaching the confidentiality of their Personal Information. Plaintiff and California Subclass members have accordingly sustained and will continue to sustain actual damages as set forth above.

508. Plaintiff and California Subclass members seek nominal, actual and statutory damages pursuant to § 56.36(b)(1) of the CMIA.

509. Plaintiff and California Subclass members also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23, Civil Code § 56.35, and California Code of Civil Procedure § 1021.5.

COUNT 10

CALIFORNIA CUSTOMER RECORDS ACT, Cal. Civ. Code §§ 1798.80, *et seq*.

510. The California Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

511. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

512. Defendants are businesses that own, maintain, and license Personal Information, within the meaning of Cal. Civ. Code § 1798.81.5, about Plaintiff and California Subclass members.

513. Businesses that own or license computerized data that includes Personal Information are required to notify California residents when their Personal Information has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

514. Defendants are businesses that own or license computerized data that includes Personal Information as defined by Cal. Civ. Code § 1798.82.

515. Plaintiff and California Subclass members' Personal Information includes Personal Information as covered by Cal. Civ. Code § 1798.82.

516. Because Defendants reasonably believed that Plaintiff's and California Subclass members' Personal Information was acquired by unauthorized persons during the Data Breach, Defendants had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

517. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Cal. Civ. Code § 1798.82.

518. As a direct and proximate result of Defendants' violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff and California Subclass members suffered damages, as described above.

519. Plaintiff and California Subclass members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

COUNT 11

CALIFORNIA UNFAIR COMPETITION LAW, Cal. Bus. & Prof. Code §§ 17200, *et seq.*

520. The California Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

521. Defendants are each a "person" as defined by Cal. Bus. & Prof. Code §17201.

522. Defendants violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

523. Defendants' "unfair" acts and practices include:

a. Failing to implement and maintain reasonable security measures to protect Plaintiff and California Subclass members' Personal Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach. Defendants failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and the California Subclass, whose Personal Information has been compromised.

b. Failing to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, HIPAA, and California's Consumer Records Act, Cal. Civ. Code § 1798.81.5.

c. Failing to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of AMCA's inadequate security, consumers could not have reasonably avoided the harms that Defendants caused.

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

524. Defendants have engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's

Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, HIPAA, and California common law.

525. Defendants' unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and California Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq., which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff and California Subclass members' Personal Information, including by implementing and maintaining reasonable security measures and ensuring their vendors and business associates maintained reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq.;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff and California Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq.

526. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

527. As a direct and proximate result of Defendants' unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Subclass members were injured and lost money or property, the price received by Defendants for their goods and services; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

528. Defendants acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff and California Subclass members' rights. Quest's past data breaches and breaches within the medical industry put them on notice that their security and privacy protections were inadequate.

529. Plaintiff and California Subclass members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendants' unfair,

unlawful, and fraudulent business practices or use of their Personal Information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT 12

CALIFORNIA CONSUMER LEGAL REMEDIES ACT, Cal. Civ. Code §§ 1750, *et seq.*

530. The California Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

531. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq*. ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

532. Defendants are each a "person" as defined by Civil Code §§ 1761(c) and 1770, and have provided "services" as defined by Civil Code §§ 1761(b) and 1770.

533. Civil Code section 1770, subdivision (a)(5) prohibits one who is involved in a transaction from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have."

534. Civil Code section 1770, subdivision (a)(7) prohibits one who is involved in a transaction from "[r]epresenting that goods or services are of a particular standard, quality, or grade . . . if they are of another."

535. Plaintiff and California Subclass members are "consumers" as defined by Civil Code §§ 1761(d) and 1770, and have engaged in a "transaction" as defined by Civil Code §§ 1761(e) and 1770.

536. Defendants' acts and practices were intended to and did result in the sales of products and services to Plaintiff and the California Subclass members in violation of Civil Code § 1770, including, but not limited to, the following:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade when they were not;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

537. Defendants' representations and omissions were material because they were likely to and did deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

538. Had Defendants disclosed to Plaintiffs and Class members that AMCA's data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and they would have been forced to use vendors and business associates with reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and California Subclass members' Personal Information as part of the services they provided without advising Plaintiffs and California Subclass members that AMCA's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Class members' Personal Information. Accordingly, Plaintiff and California Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

539. As a direct and proximate result of Defendants' violations of California Civil Code § 1770, Plaintiff and California Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

540. Plaintiff and California Subclass members have provided notice of their claims for damages to Defendants, in compliance with California Civil Code § 1782(a).

541. Plaintiff and California Subclass members seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

CLAIMS ON BEHALF OF THE COLORADO SUBCLASS

COUNT 13

COLORADO SECURITY BREACH NOTIFICATION ACT, Colo. Rev. Stat. §§ 6-1-716, *et seq.*

542. The Colorado Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Colorado Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

543. Defendants are businesses that owns or licenses computerized data that includes Personal Information as covered by Colo. Rev. Stat. §§ 6-1-716(1)(g) and 6-1-716(2).

544. Plaintiff and Colorado Subclass members' Personal Information includes Personal Information as defined by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

545. Defendants are required to accurately notify Plaintiff and Colorado Subclass members if they become aware of a breach of their data security system in the most expedient time possible and without unreasonable delay under Colo. Rev. Stat. § 6-1-716(2).

546. Because Defendants were aware of a breach of AMCA's security system that involved Plaintiff and Colorado Subclass members' Personal Information that Defendants provided to AMCA, they had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Colo. Rev. Stat. § 6-1-716(2).

547. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Colo. Rev. Stat. § 6-1-716(2).

548. As a direct and proximate result of Defendants' violations of Colo. Rev. Stat. § 6-1-716(2), Plaintiff and Colorado Subclass members suffered damages, as described above.

549. Plaintiff and Colorado Subclass members seek relief under Colo. Rev. Stat. § 6-1-716(4), including actual damages and equitable relief.

CLAIMS ON BEHALF OF THE FLORIDA SUBCLASS

COUNT 14

FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT, Fla. Stat. §§ 501.201, *et seq.*

550. The Florida Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Florida Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

551. Plaintiff and Florida Subclass members are "consumers" as defined by Fla. Stat. § 501.203.

552. Defendants advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

553. Defendants engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Florida Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Florida Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and Florida's data security statute, F.S.A. § 501.171(2), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff and Florida Subclass members' Personal Information, including by implementing and maintaining reasonable security measures and ensuring their vendors and business associates maintained reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Florida Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and Florida's data security statute, F.S.A. § 501.171(2);

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff and Florida Subclass members' Personal Information or ensure their vendors and business associates reasonably or adequately secured such information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Florida Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and Florida's data security statute, F.S.A. § 501.171(2).

554. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

555. Had Defendants disclosed to Plaintiffs and Florida Subclass members that AMCA's data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and they would have been forced to use vendors and business associates with reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and Florida Subclass members' Personal Information as part of the services they provided without advising Plaintiffs and Florida Subclass members that AMCA's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Class members' Personal Information. Accordingly, Plaintiff and Florida Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

556. As a direct and proximate result of Defendants' unconscionable, unfair, and deceptive acts and practices, Plaintiff and Florida Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

557. Plaintiff and Florida Subclass members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages under Fla. Stat. § 501.21; declaratory and injunctive relief; reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE INDIANA SUBCLASS

COUNT 15

INDIANA UNFAIR TRADE PRACTICES ACT
Indiana Code § 24-5-0.5

558. The Indiana Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Indiana Subclass, restate and re-allege the preceding paragraphs as if fully set forth herein.

559. Defendants are each a "person" as defined by Ind. Code § 24-5-0.5-2(a)(2).

560. Defendants are each a "supplier" as defined by § 24-5-0.5-2(a)(1), because they regularly engage in or solicits "consumer transactions," within the meaning of § 24-5-0.5-2(a)(3)(A).

561. Defendants engaged in unfair, abusive, and deceptive acts, omissions, and practices in connection with consumer transactions, in violation of Ind. Code § 24-5-0.5-3(a).

562. Defendants' representations and omissions include both implicit and explicit representations.

563. Defendants' unfair, abusive, and deceptive acts, omissions, and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Indiana Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Indiana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and Indiana security breach law, Ind. Code § 24-4.9-3-3.5(c), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff and Indiana Subclass members' Personal Information, including by implementing and maintaining reasonable security measures and ensuring their vendors and business associates maintained reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Indiana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and Indiana security breach law, Ind. Code § 24-4.9-3-3.5(c);

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff and Indiana Subclass members' Personal Information or ensure their vendors and business associates reasonably or adequately secured such information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Indiana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and Indiana security breach law, Ind. Code § 24-4.9-3-3.5(c).

564. Defendants' acts and practices were "unfair" because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

565. The injury to consumers from Defendants' conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and an unwarranted risk to the safety of their Personal Information or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant number of consumers, but also because it inflicted a significant amount of harm on each consumer.

566. Consumers could not have reasonably avoided injury because Defendants' business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Defendants created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

567. Defendants' inadequate data security had no countervailing benefit to consumers or to competition.

568. Defendants' acts and practices were "abusive" for numerous reasons, including:

a. because they materially interfered with consumers' ability to understand a term or condition in a consumer transaction. Defendants' failure to disclose the inadequacies in their data security interfered with consumers' decision-making in a variety of their transactions.

b. because they took unreasonable advantage of consumers' lack of understanding about the material risks, costs, or conditions of a consumer transaction. Without knowing about the inadequacies in Defendants' data security, consumers lacked an understanding of the material risks and costs of a variety of their transactions.

c. because they took unreasonable advantage of consumers' inability to protect their own interests. Consumers could not protect their interests due to the asymmetry in information between them and Defendants concerning the state of Defendants' security.

d. because Defendants took unreasonable advantage of consumers' reasonable reliance that they were acting in their interests to secure their data. Consumers' reliance was reasonable for the reasons discussed four paragraphs below.

569. Defendants also engaged in "deceptive" acts and practices in violation of Indiana Code § 24-5-0.5-3(a) and § 24-5-0.5-3(b), including:

a. Misrepresenting that the subject of a consumer transaction has sponsorship, approval, performance, characteristics, accessories, uses, or benefits it does not have which the supplier knows or should reasonably know it does not have;

b. Misrepresenting that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not and if the supplier knows or should reasonably know that it is not;

c. Misrepresenting that the subject of a consumer transaction will be supplied to the public in greater quantity (i.e., more data security) than the supplier intends or reasonably expects.

570. Defendants intended to mislead Plaintiff and Indiana Subclass members and induce them to rely on their misrepresentations and omissions.

571. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

572. Had Defendants disclosed to Plaintiffs and Class members that AMCA's data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and they would have been forced to use vendors and business associates with reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and class members' Personal Information as part of the services they provided and for which Plaintiffs and Class members paid without advising Plaintiffs and Class members that AMCA's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Class members' Personal Information. Accordingly, Plaintiff and Class members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

573. Defendants had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extent of the Personal Information in their

possession. This duty arose because members of the public, including Plaintiff and the Indiana Subclass, repose a trust and confidence in Defendants to keep their Personal Information secure. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Indiana Subclass—and Defendants, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Defendants. Defendants' duty to disclose also arose from their:

a. Possession of exclusive knowledge regarding the security of the data in their systems and their vendors' and business associates' systems;

b. Active concealment of the state of their security; and/or

c. Incomplete representations about the security and integrity of their vendors' and business associates' computer and data systems while purposefully withholding material facts from Plaintiff and the Indiana Subclass that contradicted these representations.

574. Defendants acted intentionally, knowingly, and maliciously to violate Indiana's Deceptive Consumer Sales Act, and recklessly disregarded Plaintiff and Indiana Subclass members' rights. Quest's past data breaches and breaches within the medical industry put them on notice that their security and privacy protections were inadequate. Defendants' actions were not the result of a mistake of fact or law, honest error or judgment, overzealousness, mere negligence, or other human failing.

575. Plaintiff sent a demand for relief on behalf of the Indiana Subclass pursuant to Ind. Code § 24-5-0.5-5 on November 14, 2019. Defendants have not cured their unfair, abusive, and deceptive acts and practices, or their violations of Indiana Deceptive Consumer Sales Act were incurable.

576. Since Plaintiff provided the requisite notice, Defendants have failed to cure their violations of the Indiana Deceptive Consumer Sales Act.

577. Defendants' conduct includes incurable deceptive acts that Defendants engaged in as part of a scheme, artifice, or device with intent to defraud or mislead, under Ind. Code § 24-5-0.5-2(a)(8).

578. As a direct and proximate result of Defendants' uncured or incurable unfair, abusive, and deceptive acts or practices, Plaintiff and Indiana Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants as they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

579. Defendants' violations present a continuing risk to Plaintiff and Indiana Subclass members as well as to the general public.

580. Plaintiff and Indiana Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $500 for each non-willful violation; the greater of treble damages or $1,000 for each willful violation; restitution; reasonable attorneys' fees and costs; injunctive relief; and punitive damages.

CLAIMS ON BEHALF OF THE IOWA SUBCLASS

COUNT 16

PERSONAL INFORMATION SECURITY BREACH PROTECTION LAW, Iowa Code § 715C.2

581. The Iowa Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Iowa Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

582. Defendants are each "persons" as defined by Iowa Code § 715C.2(10).

583. Plaintiffs are each "consumers" as defined by Iowa Code § 715C.2(2).

584. Defendants are each business that own or license computerized data that includes Personal Information as defined by Iowa Code § 715C.2(1).

585. Plaintiff's and Iowa Subclass members' Personal Information includes Personal Information as covered under Iowa Code § 715C.2(1).

586. Defendants are required to accurately notify Plaintiff and Iowa Subclass members if they become aware of a breach of their data security systems in the most expeditious time possible and without unreasonable delay under Iowa Code § 715C.2(1).

587. Because Defendants were aware of a breach of their vendor AMCA's security system involving the Personal Information of Plaintiff and Iowa Subclass members that Defendants provided to AMCA, Defendants had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Iowa Code § 715C.2(1).

588. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Iowa Code § 715C.2(1).

589. Pursuant to Iowa Code § 715C.2(9), a violation of Iowa Code § 715C.2(1) is an unlawful practice pursuant to Iowa Code Ann. § 714.16(7).

590. As a direct and proximate result of Defendants' violations of Iowa Code § 715C.2(1), Plaintiff and Iowa Subclass members suffered damages, as described above.

591. Plaintiff and Iowa Subclass members seek relief under Iowa Code § 714.16(7), including actual damages and injunctive relief.

COUNT 17

IOWA PRIVATE RIGHT OF ACTION FOR CONSUMER FRAUDS ACT, Iowa Code § 714H

592. The Iowa Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Iowa Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

593. Defendants are each a "person" as defined by Iowa Code § 714H.2(7).

594. Plaintiff and Iowa Subclass members are "consumers" as defined by Iowa Code § 714H.2(3).

595. Defendants' conduct described herein related to the "sale" or "advertisement" of "merchandise" as defined by Iowa Code §§ 714H.2(2), (6), & (8).

596. Defendants engaged in unfair, deceptive, and unconscionable trade practices, in violation of the Iowa Private Right of Action for Consumer Frauds Act, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Iowa Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Iowa Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff and Iowa Subclass members' Personal Information, including by implementing and maintaining reasonable security measures and ensuring their vendors and business associates maintained reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Iowa Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff and Iowa Subclass members' Personal Information or ensure their vendors and business associates reasonably or adequately secured such information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Iowa Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA.

597. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

598. Defendants intended to mislead Plaintiff and Iowa Subclass members and induce them to rely on their misrepresentations and omissions.

599. Defendants acted intentionally, knowingly, and maliciously to violate Iowa's Private Right of Action for Consumer Frauds Act, and recklessly disregarded Plaintiff and Iowa Subclass members' rights. Quest's past data breaches and breaches within the medical industry put them on notice that their security and privacy protections were inadequate.

600. As a direct and proximate result of Defendants' unfair, deceptive, and unconscionable conduct, Plaintiff and Iowa Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

601. Plaintiff has provided the requisite notice to the Iowa Attorney General, the office of which approved the filing of this class action lawsuit pursuant to Iowa Code § 714H.7.

602. Plaintiff and Iowa Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, damages, restitution, punitive damages, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE KANSAS SUBCLASS

COUNT 18

PROTECTION OF CONSUMER INFORMATION
Kan. Stat. Ann. §§ 50-7a02(a), *et seq*.

603. The Kansas Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kansas Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

604. Defendants are each a business that owns or licenses computerized data that includes Personal Information as defined by Kan. Stat. Ann. § 50-7a02(a).

605. Plaintiff's and Kansas Subclass members' Personal Information includes Personal Information as covered under Kan. Stat. Ann. § 50-7a02(a).

606. Defendants are required to accurately notify Plaintiffs and Kansas Subclass members if they become aware of a breach of their data security systems that was reasonably likely to have caused misuse of Plaintiff's and Kansas Subclass members' Personal Information, in the most expedient time possible and without unreasonable delay under Kan. Stat. Ann. § 50-7a02(a).

607. Because Defendants were aware of a breach of their vendor AMCA's security system involving the Personal Information of Plaintiff and Kansas Subclass members that Defendants provided to AMCA and that was reasonably likely to have caused misuse of Plaintiffs' and Kansas Subclass members' Personal Information, Defendants had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Kan. Stat. Ann. § 50-7a02(a).

608. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Kan. Stat. Ann. § 50-7a02(a).

609. As a direct and proximate result of Defendants' violations of Kan. Stat. Ann. § 50-7a02(a), Plaintiff and Kansas Subclass members suffered damages, as described above.

610. Plaintiff and Kansas Subclass members seek relief under Kan. Stat. Ann. § 50-7a02(g), including equitable relief.

COUNT 19

KANSAS CONSUMER PROTECTION ACT, K.S.A. §§ 50-623, *et seq*.

611. The Kansas Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kansas Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

612. K.S.A. §§ 50-623, et seq. is to be liberally construed to protect consumers from suppliers who commit deceptive and unconscionable practices.

613. Plaintiff and Kansas Subclass members are "consumers" as defined by K.S.A. § 50-624(b).

614. The acts and practices described herein are "consumer transactions," as defined by K.S.A. § 50-624(c).

615. Defendants are a "supplier" as defined by K.S.A. § 50-624(l).

616. Defendants advertised, offered, or sold goods or services in Kansas and engaged in trade or commerce directly or indirectly affecting the people of Kansas.

617. Defendants engaged in deceptive and unfair acts or practices, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Kansas Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy

measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff and Kansas Subclass members' Personal Information, including by implementing and maintaining reasonable security measures and ensuring their vendors and business associates maintained reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff and Kansas Subclass members' Personal Information or ensure their vendors and business associates reasonably or adequately secured such information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kansas Subclass members' Personal Information, including duties imposed

by the FTC Act, 15 U.S.C. § 45, HIPAA, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b.

618. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

619. Defendants intended to mislead Plaintiff and Kansas Subclass members and induce them to rely on their misrepresentations and omissions.

620. Had Defendants disclosed to Plaintiffs and Kansas Subclass members that AMCA's data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and they would have been forced to use vendors and business associates with reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and Kansas Subclass members' Personal Information as part of the services they provided without advising Plaintiffs and Kansas Subclass members that AMCA's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Kansas Subclass members' Personal Information. Accordingly, Plaintiff and Kansas Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

621. Defendants also engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of K.S.A. § 50-627, including:

a. Knowingly taking advantage of the inability of Plaintiff and Kansas Subclass members to reasonably protect their interests, due to their lack of knowledge, K.S.A. § 50-627(b)(1)); and

b. Requiring Plaintiff and Kansas Subclass members to enter into a consumer transaction on terms that Defendants knew were substantially one-sided in favor of Defendants, K.S.A. § 50-627(b)(5)).

622. Plaintiff and Kansas Subclass members had unequal bargaining power with respect to their ability to control the security and confidentiality of their Personal Information in Defendants' possession.

623. The above unfair, deceptive, and unconscionable practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kansas Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

624. Defendants acted intentionally, knowingly, and maliciously to violate Kansas's Consumer Protection Act, and recklessly disregarded Plaintiff and Kansas Subclass members' rights. Quest's past data breaches and breaches within the medical industry put them on notice that their security and privacy protections were inadequate.

625. As a direct and proximate result of Defendants' unfair, deceptive, and unconscionable trade practices, Plaintiff and Kansas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

626. Plaintiff and Kansas Subclass members seek all monetary and non-monetary relief allowed by law, including civil penalties or actual damages (whichever is greater), under K.S.A. §§ 50-634 and 50-636; injunctive relief; restitution; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE KENTUCKY SUBCLASS

COUNT 20

KENTUCKY COMPUTER SECURITY BREACH NOTIFICATION ACT, Ky. Rev. Stat. Ann. §§ 365.732, *et seq.*

627. The Kentucky Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kentucky Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

628. Defendants are each a business that holds computerized data that includes Personal Information as defined by Ky. Rev. Stat. Ann. § 365.732(2).

629. Plaintiff's and Kentucky Subclass members' Personal Information includes Personal Information as covered under Ky. Rev. Stat. Ann. § 365.732(2).

630. Defendants are required to accurately notify Plaintiff and Kentucky Subclass members if they become aware of a breach of their data security systems that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Kentucky Subclass members' Personal Information, in the most expedient time possible and without unreasonable delay under Ky. Rev. Stat. Ann. § 365.732(2).

631. Because Defendants were aware of a breach of their vendor AMCA's security system involving the Personal Information of Plaintiff and Kentucky Subclass members that Defendants provided to AMCA that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Kentucky Subclass members' Personal Information, Defendants had an

obligation to disclose the data breach in a timely and accurate fashion as mandated by Ky. Rev. Stat. Ann. § 365.732(2).

632. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Ky. Rev. Stat. Ann. § 365.732(2).

633. As a direct and proximate result of Defendants' violations of Ky. Rev. Stat. Ann. § 365.732(2), Plaintiff and Kentucky Subclass members suffered damages, as described above.

634. Plaintiff and Kentucky Subclass members seek relief under Ky. Rev. Stat. Ann. § 446.070, including actual damages.

COUNT 21

KENTUCKY CONSUMER PROTECTION ACT, Ky. Rev. Stat. §§ 367.110, *et seq*.

635. The Kentucky Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kentucky Subclass, restate and re-allege the preceding paragraphs as if fully set forth herein.

636. Defendants are each a "person" as defined by Ky. Rev. Stat. § 367.110(1).

637. Defendants advertised, offered, or sold goods or services in Kentucky and engaged in "trade" or "commerce" directly or indirectly affecting the people of Kentucky, as defined by Ky. Rev. Stat. 367.110(2).

638. Defendants engaged in unfair, false, misleading, deceptive, and unconscionable acts or practices, in violation of Ky. Rev. Stat. § 367.170, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Kentucky Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kentucky Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff and Kentucky Subclass members' Personal Information, including by implementing and maintaining reasonable security measures and ensuring their vendors and business associates maintained reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kentucky Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff and Kentucky Subclass members' Personal Information or ensure their vendors and business associates reasonably or adequately secured such information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of

Plaintiff and Kentucky Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA.

639. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

640. Defendants intended to mislead Plaintiff and Kentucky Subclass members and induce them to rely on their misrepresentations and omissions.

641. Plaintiff and Kentucky Subclass members purchased goods or services for personal, family, or household purposes and suffered ascertainable losses of money or property as a result of Defendants' unlawful acts and practices.

642. The above unlawful acts and practices by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kentucky Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

643. Defendants acted intentionally, knowingly, and maliciously to violate Kentucky's Consumer Protection Act, and recklessly disregarded Plaintiff and Kentucky Subclass members' rights. Quest's past data breaches and breaches within the medical industry put them on notice that their security and privacy protections were inadequate.

644. As a direct and proximate result of Defendants' unlawful acts and practices, Plaintiff and Kentucky Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and

expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

645. Plaintiff and Kentucky Subclass members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution or other equitable relief, injunctive relief, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE MICHIGAN SUBCLASS

COUNT 22

MICHIGAN IDENTITY THEFT PROTECTION ACT, Mich. Comp. Laws Ann. §§ 445.72, *et seq.*

646. The Michigan Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Michigan Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

647. Defendants are each a business that owns or licenses computerized data that includes Personal Information as defined by Mich. Comp. Laws Ann. § 445.72(1).

648. Plaintiff's and Michigan Subclass members' Personal Information includes Personal Information as covered under Mich. Comp. Laws Ann. § 445.72(1).

649. Defendants are required to accurately notify Plaintiff and Michigan Subclass members if they discover a security breach, or receive notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), without unreasonable delay under Mich. Comp. Laws Ann. § 445.72(1).

650. Defendants are required to provide notice that is written in a "clear and conspicuous manner." Mich. Comp. Laws Ann. § 445.72(6).

651. Because Defendants discovered a security breach and had notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by

unauthorized persons) of their vendor AMCA's security systems involving the Personal Information of Plaintiff and Michigan Subclass members that Defendants provided to AMCA, Defendants had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Mich. Comp. Laws Ann. § 445.72(4).

652. By failing to disclose the Data Breach in a timely and accurate manner and provide notice clearly and conspicuously, Defendants violated Mich. Comp. Laws Ann. § 445.72(4).

653. As a direct and proximate result of Defendants' violations of Mich. Comp. Laws Ann. § 445.72(4), Plaintiff and Michigan Subclass members suffered damages, as described above.

654. Plaintiff and Michigan Subclass members seek relief under Mich. Comp. Laws Ann. § 445.72(13), including a civil fine.

COUNT 23

MICHIGAN CONSUMER PROTECTION ACT,
Mich. Comp. Laws Ann. §§ 445.903, *et seq*.

655. The Michigan Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Michigan Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

656. Defendants and Michigan Subclass members are "persons" as defined by Mich. Comp. Laws Ann. § 445.903(d).

657. Defendants advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.903(g)

658. Defendants engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including:

a. Representing that their goods and services have characteristics, uses, and benefits that they do not have, in violation of Mich. Comp. Laws Ann. § 445.903(1)(c);

b. Representing that their goods and services are of a particular standard or quality if they are of another in violation of Mich. Comp. Laws Ann. § 445.903(1)(e);

c. Defendants advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.903(g).

d. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is, in violation of Mich. Comp. Laws Ann. § 445.903(1)(bb); and

e. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive matter, in violation of Mich. Comp. Laws Ann. § 445.903(1)(cc).

659. Defendants' unfair, unconscionable, and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Michigan Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Michigan Subclass members' Personal Information,

including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff and Michigan Subclass members' Personal Information, including by implementing and maintaining reasonable security measures and ensuring their vendors and business associates maintained reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Michigan Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff and Michigan Subclass members' Personal Information or ensure their vendors and business associates reasonably or adequately secured such information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Michigan Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA.

660. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

661. Defendants intended to mislead Plaintiff and Michigan Subclass members and induce them to rely on their misrepresentations and omissions.

662. Defendants acted intentionally, knowingly, and maliciously to violate Michigan's Consumer Protection Act, and recklessly disregarded Plaintiff and Michigan Subclass members' rights. Quest's past data breaches and breaches within the medical industry put them on notice that their security and privacy protections were inadequate.

663. As a direct and proximate result of Defendants' unfair, unconscionable, and deceptive practices, Plaintiff and Michigan Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

664. Plaintiff and Michigan Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $250, restitution, injunctive relief, and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE MISSOURI SUBCLASS

COUNT 24

MISSOURI MERCHANDISING PRACTICES ACT, Mo. Rev. Stat. §§ 407.010, *et seq*.

665. The Missouri Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Missouri Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

666. Defendants are each a "person" as defined by Mo. Rev. Stat. § 407.010(5).

667. Defendants advertised, offered, or sold goods or services in Missouri and engaged in trade or commerce directly or indirectly affecting the people of Missouri, as defined by Mo. Rev. Stat. § 407.010(4), (6) and (7).

668. Defendants engaged in unlawful, unfair, and deceptive acts and practices, in connection with the sale or advertisement of merchandise in trade or commerce, in violation of Mo. Rev. Stat. § 407.020(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Missouri Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Missouri Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff and Missouri Subclass members' Personal Information, including by implementing and maintaining reasonable security measures and ensuring their vendors and business associates maintained reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Missouri Subclass members'

Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff and Missouri Subclass members' Personal Information or ensure their vendors and business associates reasonably or adequately secured such information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Missouri Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA.

669. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

670. Defendants intended to mislead Plaintiff and Missouri Subclass members and induce them to rely on its misrepresentations and omissions.

671. Defendants acted intentionally, knowingly, and maliciously to violate Missouri's Merchandising Practices Act, and recklessly disregarded Plaintiff and Missouri Subclass members' rights. Quest's past data breaches and breaches within the medical industry put them on notice that their security and privacy protections were inadequate.

672. As a direct and proximate result of Defendants' unlawful, unfair, and deceptive acts and practices, Plaintiff and Missouri Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including losses from fraud and identity theft; costs for credit monitoring and identity protection

services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

673. Plaintiff and Missouri Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, restitution, punitive damages, attorneys' fees and costs, injunctive relief, and any other appropriate relief.

CLAIMS ON BEHALF OF THE NEW HAMPSHIRE SUBCLASS

COUNT 25

NOTICE OF SECURITY BREACH
N.H. Rev. Stat. Ann. §§ 359-C:20(I)(A), *et seq.*

674. The New Hampshire Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New Hampshire Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

675. Defendants are each a business that owns or licenses computerized data that includes Personal Information as defined by N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

676. Plaintiff's and New Hampshire Subclass members' Personal Information includes Personal Information as covered under N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

677. Defendants are required to accurately notify Plaintiff and New Hampshire Subclass members if Defendants become aware of a breach of its data security systems in which misuse of Personal Information has occurred or is reasonably likely to occur, as soon as possible under N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

678. Because Defendants were aware of a security breach of AMCA's security systems involving the Personal Information of Plaintiff and New Hampshire Subclass members that Defendants provided to AMCA and in which misuse of Personal Information has occurred or is

reasonably likely to occur, Defendants had an obligation to disclose the data breach in a timely and accurate fashion as mandated by N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

679. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

680. As a direct and proximate result of Defendants' violations of N.H. Rev. Stat. Ann. § 359-C:20(I)(a), Plaintiff and New Hampshire Subclass members suffered damages, as described above.

681. Plaintiff and New Hampshire Subclass members seek relief under N.H. Rev. Stat. Ann. § 359-C:21(I), including actual damages and injunctive relief.

COUNT 26

NEW HAMPSHIRE CONSUMER PROTECTION ACT, N.H.R.S.A. §§ 358-A, *et seq.*

682. The New Hampshire Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New Hampshire Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

683. Defendants are each a "person" under the New Hampshire Consumer Protection Act.

684. Defendants advertised, offered, or sold goods or services in New Hampshire and engaged in trade or commerce directly or indirectly affecting the people of New Hampshire, as defined by N.H.R.S.A. § 358-A:1.

685. Defendants engaged in unfair and deceptive acts or practices in the ordinary conduct of its trade or business, in violation of N.H.R.S.A. § 358-A:2, including:

a. Representing that their goods or services have characteristics, uses, or benefits that they do not have in violation of N.H.R.S.A. § 358-A:2.V;

b. Representing that their goods or services are of a particular standard or quality if they are of another in violation of N.H.R.S.A. § 358-A:2.VII; and

c. Advertising their goods or services with intent not to sell them as advertised in violation of N.H.R.S.A. § 358-A:2.IX.

686. Defendants' unfair and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and New Hampshire Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Hampshire Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff and New Hampshire Subclass members' Personal Information, including by implementing and maintaining reasonable security measures and ensuring their vendors and business associates maintained reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Hampshire Subclass

members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPPA;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff and New Hampshire Subclass members' Personal Information or ensure their vendors and business associates reasonably or adequately secured such information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Hampshire Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA.

687. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

688. Defendants acted intentionally, knowingly, and maliciously to violate New Hampshire's Consumer Protection Act, and recklessly disregarded Plaintiff and New Hampshire Subclass members' rights. Quest's past data breaches and breaches within the medical industry put them on notice that their security and privacy protections were inadequate. Defendants' acts and practices went beyond the realm of strictly private transactions.

689. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiff and New Hampshire Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages; losses from fraud and identity theft, including costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity;

loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

690. Plaintiff and New Hampshire Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, punitive damages, equitable relief (including injunctive relief), restitution, civil penalties, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE NEW JERSEY SUBCLASS

COUNT 27

NEW JERSEY CUSTOMER SECURITY BREACH DISCLOSURE ACT, N.J.S.A. §§ 56:8-163, *et seq.*

691. The New Jersey Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New Jersey Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

692. Defendants are each a business that conducts business in New Jersey under N.J.S.A. § 56:8-163(a).

693. Plaintiff's and New Jersey Subclass members' Personal Information includes Personal Information covered under N.J.S.A. §§ 56:8-163, *et seq*.

694. Under N.J.S.A. § 56:8-163(a), "[a]ny business that conducts business in New Jersey. . . shall disclose any breach of security of [] computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person."

695. Because Defendants discovered a breach of AMCA's security system involving the Personal Information of Plaintiff and New Jersey Subclass members that Defendants provided to AMCA in which such Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Personal Information was not secured, Defendants had an

obligation to disclose the Data Breach in a timely and accurate fashion as mandated under N.J.S.A. §§ 56:8-163, *et seq.*

696. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated N.J.S.A. § 56:8-163(a).

697. As a direct and proximate result of Defendants' violations of N.J.S.A. § 56:8-163(a), Plaintiff and New Jersey Subclass members suffered the damages described above.

698. Plaintiff and New Jersey Subclass members seek relief under N.J.S.A. § 56:8-19, including treble damages, attorneys' fees and costs, and injunctive relief.

CLAIMS ON BEHALF OF THE NEW YORK SUBCLASS

COUNT 28

NEW YORK GENERAL BUSINESS LAW, N.Y. Gen. Bus. Law §§ 349, *et seq.*

699. The New York Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New York Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

700. Defendants engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and New York Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy

measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New York Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff and New York Subclass members' Personal Information, including by implementing and maintaining reasonable security measures and ensuring their vendors and business associates maintained reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New York Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff and New York Subclass members' Personal Information or ensure their vendors and business associates reasonably or adequately secured such information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New York Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA.

701. Plaintiff and New York Subclass members were deceived in New York. They also transacted with Defendants in New York by utilizing Defendants' services in New York.

702. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

703. Defendants acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff and New York Subclass members' rights. Quest's past data breaches and breaches within the medical industry put them on notice that their security and privacy protections were inadequate.

704. As a direct and proximate result of Defendants' deceptive and unlawful acts and practices, Plaintiff and New York Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

705. Defendants' deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the hundreds of thousands, if not millions, of New Yorkers affected by the Data Breach.

706. The above deceptive and unlawful practices and acts by Defendants caused substantial injury to Plaintiff and New York Subclass members that they could not reasonably avoid.

707. Plaintiff and New York Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, restitution, injunctive relief, and attorney's fees and costs.

CLAIMS ON BEHALF OF THE OHIO SUBCLASS

COUNT 29

OHIO CONSUMER SALES PRACTICES ACT, Ohio Rev. Code §§ 1345.01, *et seq*.

708. The Ohio Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Ohio Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

709. Plaintiff and Ohio Subclass members are "persons," as defined by Ohio Rev. Code § 1345.01(B).

710. Defendants were each a "supplier" engaged in "consumer transactions," as defined by Ohio Rev. Code §§ 1345.01(A) & (C).

711. Defendants advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

712. Defendants engaged in unfair and deceptive acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code §§ 1345.02, including:

a. Representing that their goods, services, and intangibles had performance characteristics, uses, and benefits that they did not have, in violation of Ohio Rev. Code § 1345.02(B)(1); and

b. Representing that their goods, services, and intangibles were of a particular standard or quality when they were not, in violation of Ohio Rev. Code § 1345(B)(2).

713. Defendants engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code Ann. § 1345.03, including:

a. Knowingly taking advantage of the inability of Plaintiff and Ohio Subclass members to reasonably protect their interest because of their ignorance of the issues discussed herein (Ohio Rev. Code Ann. § 1345.03(B)(1)); and

b. Requiring Plaintiff and Ohio Subclass members to enter into a consumer transaction on terms that Defendants knew were substantially one-sided in favor of Defendants (Ohio Rev. Code Ann. § 1345.03(B)(5)).

714. Defendants' unfair, deceptive, and unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Ohio Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff and Ohio Subclass members' Personal Information, including by implementing and maintaining reasonable security measures and ensuring their vendors and business associates maintained reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff and Ohio Subclass members' Personal Information or ensure their vendors and business associates reasonably or adequately secured such information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA.

715. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

716. Defendants intended to mislead Plaintiff and Ohio Subclass members and induce them to rely on their misrepresentations and omissions.

717. Defendants acted intentionally, knowingly, and maliciously to violate Ohio's Consumer Sales Practices Act, and recklessly disregarded Plaintiff and Ohio Subclass members' rights. Quest's past data breaches and breaches within the medical industry put them on notice that their security and privacy protections were inadequate.

718. Defendants' unfair, deceptive, and unconscionable acts and practices complained of herein affected the public interest, including the many Ohioans affected by the Data Breach.

719. As a direct and proximate result of Defendants' unfair, deceptive, and unconscionable acts and practices, Plaintiff and Ohio Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

720. Plaintiff and Ohio Subclass members seek all monetary and non-monetary relief allowed by law, including declaratory and injunctive relief, the greater of actual and treble damages or statutory damages, attorneys' fees and costs, and any other appropriate relief.

COUNT 30

OHIO DECEPTIVE TRADE PRACTICES ACT,
Ohio Rev. Code §§ 4165.01, *et seq*.

721. The Ohio Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Ohio Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

722. Defendants, Plaintiff, and Ohio Subclass members are each a "person," as defined by Ohio Rev. Code § 4165.01(D).

723. Defendants advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

724. Defendants engaged in deceptive trade practices in the course of its business and vocation, in violation of Ohio Rev. Code § 4165.02, including:

a. Representing that their goods and services have characteristics, uses, benefits, or qualities that they do not have, in violation of Ohio Rev. Code § 4165.02(A)(7);

b. Representing that their goods and services are of a particular standard or quality when they are of another, in violation of Ohio Rev. Code § 4165.02(A)(9); and

c. Advertising their goods and services with intent not to sell them as advertise, in violation of Ohio Rev. Code § 4165.02(A)(11).

725. Defendants' deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Ohio Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff and Ohio Subclass members' Personal Information, including by implementing and maintaining reasonable security measures and ensuring their vendors and business associates maintained reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff and Ohio Subclass members' Personal Information or ensure their vendors and business associates reasonably or adequately secured such information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA.

726. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

727. Defendants intended to mislead Plaintiff and Ohio Subclass members and induce them to rely on their misrepresentations and omissions.

728. Defendants acted intentionally, knowingly, and maliciously to violate Ohio's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Ohio Subclass members' rights. Quest's past data breaches and breaches within the medical industry put them on notice that their security and privacy protections were inadequate.

729. As a direct and proximate result of Defendants' deceptive trade practices, Plaintiff and Ohio Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

730. Plaintiff and Ohio Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages, restitution, attorneys' fees, and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE PENNSYLVANIA SUBCLASS

COUNT 31

PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW, 73 Pa. Cons. Stat. §§ 201-2 & 201-3, *et seq*.

731. The Pennsylvania Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Pennsylvania Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

732. Defendants are a "person", as meant by 73 Pa. Cons. Stat. § 201-2(2).

733. Plaintiff and Pennsylvania Subclass members purchased goods and services in "trade" and "commerce," as meant by 73 Pa. Cons. Stat. § 201-2(3), primarily for personal, family, and/or household purposes.

734. Defendants engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of its trade and commerce in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including:

a. Representing that their goods and services have characteristics, uses, benefits, and qualities that they do not have (73 Pa. Stat. Ann. § 201-2(4)(v));

b. Representing that their goods and services are of a particular standard or quality if they are another (73 Pa. Stat. Ann. § 201-2(4)(vii)); and

c. Advertising their goods and services with intent not to sell them as advertised (73 Pa. Stat. Ann. § 201-2(4)(ix)).

735. Defendants' unfair or deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Pennsylvania Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Pennsylvania Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff and Pennsylvania Subclass members' Personal Information, including by implementing and maintaining reasonable security measures and ensuring their vendors and business associates maintained reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Pennsylvania Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff and Pennsylvania Subclass members' Personal Information or ensure their vendors and business associates reasonably or adequately secured such information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff

and Pennsylvania Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA.

736. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

737. Defendants intended to mislead Plaintiff and Pennsylvania Subclass members and induce them to rely on their misrepresentations and omissions.

738. Had Defendants disclosed to Plaintiffs and Pennsylvania Subclass members that AMCA's data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and they would have been forced to use vendors and business associates with reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and Pennsylvania Subclass members' Personal Information as part of the services they provided without advising Plaintiffs and Pennsylvania Subclass members that AMCA's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Pennsylvania Subclass members' Personal Information. Accordingly, Plaintiff and Pennsylvania Subclass members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

739. Defendants acted intentionally, knowingly, and maliciously to violate Pennsylvania Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff and Pennsylvania Subclass members' rights.

740. As a direct and proximate result of Defendants' unfair methods of competition and unfair or deceptive acts or practices and Plaintiff's and Pennsylvania Subclass members' reliance on them, Plaintiff and Pennsylvania Subclass members have suffered and will continue to suffer

injury, ascertainable losses of money or property, and monetary and non-monetary damages; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

741. Plaintiff and Pennsylvania Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $100 (whichever is greater), treble damages, restitution, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

CLAIMS ON BEHALF OF THE TENNESSEE SUBCLASS

COUNT 32

TENNESSEE PERSONAL CONSUMER INFORMATION RELEASE ACT, Tenn. Code Ann. §§ 47-18-2107, *et seq*.

742. The Tennessee Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Tennessee Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

743. Defendants are each a business that owns or licenses computerized data that includes Personal Information as defined by Tenn. Code Ann. § 47-18-2107(a)(3).

744. Plaintiff's and Tennessee Subclass members' Personal Information includes Personal Information as covered under Tenn. Code Ann. § 47-18- 2107(a)(4)(A).

745. Defendants are required to accurately notify Plaintiff and Tennessee Subclass members following discovery or notification of a breach of their data security system in which unencrypted Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person, in the most expedient time possible and without unreasonable delay under Tenn. Code Ann. § 47-18-2107(b).

746. Because Defendants discovered a breach of AMCA's security system involving the Personal Information of Plaintiff and Tennessee Subclass members that Defendants provided to AMCA in which unencrypted Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person, Defendants had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Tenn. Code Ann. § 47-18-2107(b).

747. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Tenn. Code Ann. § 47-18-2107(b).

748. As a direct and proximate result of Defendants' violations of Tenn. Code Ann. § 47-18-2107(b), Plaintiff and Tennessee Subclass members suffered damages, as described above.

749. Plaintiff and Tennessee Subclass members seek relief under Tenn. Code Ann. §§ 47-18-2107(h), 47-18-2104(d), and 47-18-2104(f), including actual damages, injunctive relief, and treble damages.

REQUESTS FOR RELIEF

Plaintiffs, individually and on behalf of members of the Class and Subclasses, as applicable, respectfully requests that the Court enter judgment in their favor and against Defendants, as follows:

1. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are proper class representatives; and appoint Plaintiffs' Co-Lead and Co-Liaison Counsel as Class Counsel;

2. That the Court grant permanent injunctive relief to prohibit Defendants from continuing to engage in the unlawful acts, omissions, and practices described herein;

3. That the Court award Plaintiffs and Class and Subclass members compensatory, consequential, and general damages in an amount to be determined at trial;

4. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of their unlawful acts, omissions, and practices;

5. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

6. That Plaintiffs be granted the declaratory relief sought herein;

7. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

8. That the Court award pre- and post-judgment interest at the maximum legal rate; and

9. That the Court grant all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial on all claims so triable.

CARELLA, BYRNE, CECCHI,
OLSTEIN, BRODY & AGNELLO, P.C.
Interim Lead Counsel for Plaintiffs

By: /s/ James E. Cecchi
JAMES E. CECCHI

Dated: November 15, 2019

Christopher A. Seeger
Parvin Aminolroaya
Jennifer Scullion
SEEGER WEISS LLP
55 Challenger Road, 6th Floor
Ridgefield Park, New Jersey 07660
(973) 639-9100

Norman E. Siegel
Barrett J. Vahle
J. Austin Moore
STUEVE SIEGEL HANSON LLP

E. Michelle Drake
BERGER MONTAGUE PC
43 SE Main Street, Suite 505
Minneapolis, Minnesota 55414
(612) 594-5999

Jason T. Dennett
Kim D. Stephens
Cecily C. Shiel
TOUSLEY BRAIN STEPHENS, PLLC
1700 Seventh Avenue, Suite 2200
Seattle, Washington 98101

460 Nichols Road, Suite 200
Kansas City, Missouri 64112
(816) 714-7100

Jason L. Lichtman
Sean A. Petterson
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
250 Hudson Street, 8th Floor
New York, New York 10013
(212) 355-9500

Quest Track Co-Lead Counsel

(206) 682-5600

Timothy G. Blood
Thomas J. O'Reardon II
BLOOD HURST & O'REARDON, LLP
502 West Broadway, Suite 1490
San Diego, California 92101
(619) 338-1101

Todd S. Garber
Jeremiah Frei-Pearson
D. Greg Blankinship
Chantal Khalil
FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP
445 Hamilton Avenue, Suite 605
White Plains, New York 10601
(914) 298-3281

Quest Track Steering Committee